OPAP
DEC 0 6 2010
PATENT & TRADEMARK OFFICE
IAP8

PATENT
7251/94662

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Applicants: MAIL et al.

For: OPTIMALLY ADAPTING MULTIMEDIA CONTENT FOR MOBILE SUBSCRIBER DEVICE PLAYBACK

Serial No.: 10/589,417

371(c) Date: 7 November 2006

Group Art Unit: 2442

Examiner: Michael W. Chao

APPELLANTS' BRIEF ON APPEAL

Mail Stop Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

Dear Sir or Madam:

This is an Appeal from the Final Office Action mailed 20 May 2010 that rejected all of the pending claims. A Notice of Appeal and a Request for Pre-Appeal Brief Review were filed on 13 September 2010. The 4 November 2010 Notice of Panel Decision from Pre-Appeal Brief Review maintained the rejection of all pending claims. The applicable fee accompanies this Appeal Brief. Should there be any deficiency in fees in connection with this Appeal, the Commissioner is hereby authorized to charge any such deficiency in fees to Deposit Account 23-0920.

12/08/2010 CCHAU1 00000023 230920 10589417
01 FC:1402 540.00 DA

1. REAL PARTY IN INTEREST

The real parties in interest are NDS LIMITED and its parent company NDS Group Limited, both companies organized under the laws of England, and both with a place of business at One London Road, Staines, Middlesex TW18 4EX, United Kingdom.

2. RELATED APPEALS AND INTERFERENCES

There are no appeals, interferences, or judicial proceedings related to, directly affecting or affected by, or having a bearing on the Board's decision in the captioned Appeal.

3. STATUS OF CLAIMS

Claims 1, 3-14, 17-21, 26-29, 31-42, 45-49 and 58-60 are currently pending, stand rejected and are being appealed. That is,

1:	currently pending, rejected, subject of this appeal
2:	cancelled without prejudice
3-14:	currently pending, rejected, subject of this appeal
15-16:	cancelled without prejudice
17-21:	currently pending, rejected, subject of this appeal
22-25:	cancelled without prejudice
26-29:	currently pending, rejected, subject of this appeal
30:	cancelled without prejudice
31-42:	currently pending, rejected, subject of this appeal
43-44:	cancelled without prejudice

45-49: currently pending, rejected, subject of this appeal

50-57: cancelled without prejudice

58-60: currently pending, rejected, subject of this appeal

4. STATUS OF AMENDMENTS

No amendments were filed subsequent to the pending rejection.

5. SUMMARY OF CLAIMED SUBJECT MATTER

Citations are to the application as filed, which is included in the Evidence Appendix, tab 1.

Independent Claim 1 recites a method for distributing multimedia content. (*See e.g.* Abstract). The method comprises storing an item of multimedia content as stored multimedia content at a multimedia message center (MMSC). (*See e.g.* 9:21-22). It further comprises transcoding the multimedia content for playback on a first multimedia device, thereby producing a firstly transcoded version of the multimedia content. (*See e.g.* 10:10-12). It further comprises generating a content ID of the firstly transcoded version of the multimedia content. (*See e.g.* 10:12-13). It further comprises storing the content ID of the firstly transcoded version of the multimedia content, as a stored first content ID, in association with the stored multimedia content. (*See e.g.* 10:13-14). It further comprises receiving, at the MMSC via a multimedia message service (MMS) message, an instruction to forward the item of multimedia content to a second multimedia device. (*See e.g.* 10:26-28). The instruction comprises a copy of the firstly transcoded version of the multimedia content. (*See*

e.g. 10:28-29). The method further comprises performing the following in response to the instruction: accessing the stored multimedia content using the stored first content ID of the firstly transcoded version of the multimedia content (*see e.g.* 11:5-6), and transcoding the stored multimedia content for playback on the second multimedia device (*see e.g.* 11:11-12). The accessing comprises generating a received content ID of the copy of the firstly transcoded version of the multimedia content (*see e.g.* 10:18 and 11:7-9), and looking up the stored multimedia content by comparing the received content ID with the stored first content ID (*see e.g.* 11:9-10).

Independent Claim 26 recites a multimedia content distribution system. (*See e.g.* Figs. 1A-1D). The system comprises an MMS server (*see e.g.* MMS server 202, Figs. 2 and 3), an MMS relay (*see e.g.* MMS relay 204, Figs. 2 and 3), a transcoder (*see e.g.* transcoder 208, Figs. 2 and 3), and a DRM server (*see e.g.* DRM server 210, Figs. 2 and 3), where at least one is implemented at least partially in hardware (*see e.g.* 15:23-26). The MMS server, MMS relay, transcoder and DRM server are individually or cooperatively operative to store an item of multimedia content as stored multimedia content (*see e.g.* 9:21-22), transcode the multimedia content for playback on a first multimedia device, thereby producing a firstly transcoded version of the multimedia content (*see e.g.* 10:10-12), generate a content ID of the firstly transcoded version of the multimedia content (*see e.g.* 10:12-13), store the content ID of the firstly transcoded version of the multimedia content, as a stored first content ID, in association with the stored multimedia content (*see e.g.* 10:13-14), receive an instruction, via a multimedia message service (MMS) message, to forward the item of multimedia content to a second multimedia device (*see e.g.* 10:26-28) [the instruction

comprising a copy of the firstly transcoded version of the multimedia content (*see e.g.* 10:28-29)], and performing the following in response to the instruction: accessing the stored multimedia content using the stored first content ID of the firstly transcoded version of the multimedia content (*see e.g.* 11:5-6), and transcoding the stored multimedia content for playback on the second multimedia device (*see e.g.* 11:11-12). The accessing comprises generating a received content ID of the copy of the firstly transcoded version of the multimedia content (*see e.g.* 10:18 and 11:7-9), and looking up the stored multimedia content by comparing the received content ID with the stored first content ID (*see e.g.* 11:9-10).

Independent Claim 29 recites a system for distributing multimedia content. (*See e.g.* Figs. 1A-1D). The system comprises a means for storing an item of multimedia content as stored multimedia content at a multimedia message center (MMSC). (*See e.g.* 13:8, 13:25-27, MMS server 202, Figs. 2 and 3; 9:21-22). It further comprises a means for transcoding the multimedia content for playback on a first multimedia device, thereby producing a firstly transcoded version of the multimedia content. (*See e.g.* 13:14, 13:25-27, transcoder 208, Figs. 2 and 3; 10:10-12). It further comprises a means for generating a content ID of the firstly transcoded version of the multimedia content. (*See e.g.* 13:25-30, DRM server 210, Figs. 2 and 3; 10:12-13). It further comprises a means for storing the content ID of the firstly transcoded version of the multimedia content, as a stored first content ID, in association with the stored multimedia content. (*See e.g.* 13:8, 13:25-27, MMS server 202, Figs. 2 and 3; 10:13-14). It further comprises a means for receiving, at the MMSC via a multimedia message service (MMS) message, an instruction to forward

the item of multimedia content to a second multimedia device. (*See e.g.* 13:9, 13:25-27, MMS relay 204, Figs. 2 and 3; 10:26-28). The instruction comprises a copy of the firstly transcoded version of the multimedia content. (*See e.g.* 10:28-29). The method further comprises a means for performing the following in response to the instruction: accessing the stored multimedia content using the stored first content ID of the firstly transcoded version of the multimedia content (*see e.g.* 13:8, 13:25-27, MMS server 202, Figs. 2 and 3; 11:5-6), and means for transcoding the stored multimedia content for playback on the second multimedia device (*see e.g.* 13:14, 13:25-27, transcoder 208, Figs. 2 and 3; 11:11-12). The accessing comprises generating a received content ID of the copy of the firstly transcoded version of the multimedia content (*see e.g.* 13:25-30, DRM server 210, Figs. 2 and 3; 10:18 and 11:7-9), and looking up the stored multimedia content by comparing the received content ID with the stored first content ID (*see e.g.* 13:8,13:25-27, MMS server 202, Figs. 2 and 3; 11:9-10).

6. GROUNDS FOR REJECTION

Claims 1, 3-14, 29 and 31-42 stand rejected under 35 U.S.C. §103(a) as being rendered obvious by Warsta (US 2004/0181550) in view of Malik (US 7,003,551). Claims 17-21, 26-28 and 45-49 stand rejected under 35 U.S.C. §103(a) as being rendered obvious by Warsta in view of Malik, and further in view of Kobata (US 2002/0077986). Claims 58-60 stand rejected under 35 U.S.C. §103(a) as being rendered obvious by Warsta in view of Malik, and further in view of Mattis (US 6,128,623).

7. ARGUMENT – CLAIMS 1, 3-14, 17-21, 26-29, 31-42, 45-49 AND 58-60 - THE REFERENCES DO *NOT* SUGGEST WHAT IS CLAIMED: TRANSCODING AN ORIGINAL VERSION OF CONTENT FOR COMPATIBILITY WITH A SECOND DEVICE, RATHER THAN TRANSCODING A VERSION THAT PREVIOUSLY WAS TRANSCODED FOR COMPATIBILITY WITH A FIRST DEVICE

A. BACKGROUND

By way of background, the present invention relates to an area of technology in which the "Multimedia Message Service (MMS) provides for the transmission of graphics, video clips, sound files and text messages over wireless networks." (Appl. 1:16-17, Tab 1 of Evid. App.). Typically, this is implemented using MMS Centers (MMSCs) that store and forward "multimedia messages from providers of multimedia content to mobile subscribers, as well as multimedia message exchange between mobile subscribers." (Appl. 1:19-21, Tab 1 of Evid. App.). One challenge is adapting the multimedia content for a wide variety of mobile subscriber devices. "Adapting content currently incurs a relatively large computational expense when transcoding content for different playback environments." (Appl. 1:28-30, Tab 1 of Evid. App.).

B. THE CLAIMS RECITE TRANSCODING THE ORIGINAL VERSION OF CONTENT FOR PLAYBACK ON A SECOND DEVICE

Claim 1 recites, *inter alia*,

> storing an item of multimedia content as *stored multimedia content...*;
>
> ...transcoding said multimedia content for playback on a first multimedia device, thereby producing a firstly transcoded version...;
>
> * * *

receiving... an instruction to forward said item of multimedia content to a second multimedia device, said instruction comprising a copy of said firstly transcoded version...;

* * *

...in response to said instruction:

* * *

transcoding *said stored multimedia content* for playback on said second multimedia device.

[emphasis added]. That is, an item of multimedia content is stored, and then is identified in the claims as the *stored multimedia content*. The content also is transcoded to be compatible with a first device (such as a mobile subscriber device of a particular user), and that transcoded version of the content is identified in the claims as the firstly transcoded version. An instruction that includes the firstly transcoded version is received (such as from the mobile subscriber device of the particular user) to forward the content to a second device (such as a second mobile subscriber device possibly belonging to a different user). In response to that instruction, the *original* version of the stored content (the claimed *stored multimedia content*) is transcoded for playback on the second device. That is, the firstly transcoded version that is received with the instruction might not be compatible with the second device, and it is the original version (rather than the firstly transcoded version that is received with the instruction) that is transcoded to be compatible with the second device.

Claims 1, 26 and 29 are the only independent claims. Claims 26 and 29 have substantially identical limitations as those quoted above from claim 1. Therefore, all of the claims directly or indirectly include the claim limitations discussed above.

The quoted "said stored multimedia content" is the original version of the content introduced in the initial storing step of claim 1. It is *not* the firstly transcoded version of that content that was included with the instruction to forward the content to the second device.

The significance of transcoding the original version (the *stored multimedia content*), rather than the firstly transcoded version that was attached to the instruction to forward the content to the second device, was explained in the Background section of the application:

> when content that was previously transcoded for playback on one mobile subscriber device is sent from the mobile subscriber device to another mobile subscriber device, the transcoded content is typically transcoded again by the MMSC for playback on the intended recipient's device. This typically results in a lower playback quality than would be the case if the original content was transcoded for playback on the intended recipient's device.

(Appl. 1:31 – 2:5, tab 1 of Evid. App.). In the method of claim 1, this problem is overcome because the transcoded content is *not* transcoded again for compatibility with the second device. Rather, the original version of the content is transcoded for compatibility with the second device. Therefore, there is no additional reduction in quality resulting from transcoding a previously transcoded version.

C. WARSTA AND THE OTHER CITED REFERENCES DO *NOT* DISCLOSE OR SUGGEST WHAT IS CLAIMED

Warsta (included as Evid. App., tab 4) and the other references on which the rejections relied do not disclose or suggest what is claimed. If device #1 sends content for delivery to device #2, the Warsta system checks if a version of that content that is compatible with device #2 is cached. If it is not cached, the Warsta

system will transcode the content to be compatible with device #2. However, Warsta does *not* disclose or suggest that it will go back to the original version of the content, as opposed to transcoding the version sent from device #1 that already had been transcoded to be compatible with device #1. This is the very problem quoted above from the background section of the captioned application.

In this regard, Malik (included as Evid. App., tab 5) and the other references do not add anything to the Warsta disclosure. In particular, Malik concerns minimizing the number of duplicate copies of identical attachments to e-mail that are stored. Malik uses pointers to associate an e-mail with attachments, and it has nothing to do with transcoding to create a different version of content. (*See e.g.* Malik Abstract, tab 5 of Evid. App.).

In addressing the claim limitation that recites transcoding the original version of the content for playback on the second device, the bottom of page 6 and top of page 7 of the 20 May 2010 Final Office Action (included as Evid. App., tab 2) cited language in paragraphs 24 and 29 of Warsta. That cited language merely indicated that the Warsta system would check if it already had *stored* a version of the content that was adapted for playback on the "second device." That cited language and any other language in Warsta or in any of the other cited references does *not* disclose or suggest that, if transcoding is required for the "second device" (i.e., if a version adapted for playback on the "second device" is not available), the original version of the content would be transcoded (as claimed). There is *no* disclosure or suggestion that the Warsta system would not do exactly what other prior art systems do in this scenario. That is, there is *no* disclosure or suggestion that the Warsta system would

not transcode the firstly transcoded version that was included in the instruction to forward the content to the second device, rather than transcoding the original version of the content as claimed.

The 29 July 2010 Advisory Action (included as Evid. App., tab 3) addressed a different claim limitation concerning *storing* the original version of the content. It did *not* address which version is transcoded in the scenario recited in the claims. It did *not* address the failure of the references to disclose or suggest the claim limitation discussed above.

A claim is not shown to be obvious by a combination of references when one of the claim limitations is not disclosed by any of those references. *See e.g. Honeywell International Inc. v. United States*, 596 F.3d 800, 810, 93 USPQ2d 1740, 1747 (Fed. Cir. 2010). In the captioned application, *none* of the references discloses or suggests transcoding the original version of the content (the "stored multimedia content") rather than the previously transcoded version (the "firstly transcoded version") that was included with the instruction to forward the content to the second device. Therefore, the combination of references does *not* render the claims obvious.

8. CLAIMS APPENDIX

An appendix is attached containing a copy of the claims involved in this appeal.

9. EVIDENCE APPENDIX

An appendix is attached containing the application as filed, the 20 May 2010 Final Office Action, the 29 July 2010 Advisory Action, Warsta (US 2004/0181550), and Malik (US 7,003,551).

10. RELATED PROCEEDINGS APPENDIX

There are no related proceedings.

Favorable consideration of this Appeal and allowance of the application are respectfully requested.

Respectfully submitted,

6 December 2010

L. Friedman
Reg. No. 37,135

HUSCH BLACKWELL LLP
WELSH KATZ
120 South Riverside Plaza, Suite 2200
Chicago, Illinois 60606
(312) 655-1500

CLAIMS APPENDIX

Claim 1: A method for distributing multimedia content, the method comprising:

storing an item of multimedia content as stored multimedia content at a multimedia message center (MMSC);

firstly transcoding said multimedia content for playback on a first multimedia device, thereby producing a firstly transcoded version of said multimedia content;

generating a content ID of said firstly transcoded version of said multimedia content;

storing said content ID of said firstly transcoded version of said multimedia content, as a stored first content ID, in association with said stored multimedia content;

receiving, at said MMSC via a multimedia message service (MMS) message, an instruction to forward said item of multimedia content to a second multimedia device, said instruction comprising a copy of said firstly transcoded version of said multimedia content; and

performing the following in response to said instruction:

accessing said stored content using said stored first content ID of said firstly transcoded version of said multimedia content, said accessing comprising:

generating a received content ID of said copy of said firstly transcoded version of said multimedia content; and

looking up said stored multimedia content by comparing said received content ID with said stored first content ID; and

transcoding said stored multimedia content for playback on said second multimedia device.

Claim 3: A method according to claim 1 wherein said storing an item of multimedia content comprises storing said item of multimedia content together with an original content identifier (ID) identifying said content.

Claim 4: A method according to claim 1 wherein said storing an item of multimedia content comprises storing said item of multimedia content together with an original content identifier (ID) that uniquely identifies said content.

Claim 5: A method according to claim 1 wherein said storing an item of multimedia content comprises storing said item of multimedia content in its original form.

Claim 6: A method according to claim 1 wherein said storing an item of multimedia content comprises storing said item of multimedia content such that said content may be partly or wholly reconstituted.

Claim 7: A method according to claim 3 and further comprising receiving said original content ID from a provider of said content.

Claim 8: A method according to claim 3 and further comprising generating said original content ID by applying either of a predefined hashing method and a predefined fingerprinting method to said content and using either of the resulting hash and fingerprint as said original content ID.

Claim 9: A method according to claim 3 and further comprising associating said original content ID with different transcoded versions of said content.

Claim 10: A method according to claim 1 and further comprising sending a notification to said first multimedia device indicating that said content is available for download to said multimedia device.

Claim 11: A method according to claim 1 and further comprising delivering said firstly transcoded content to said first multimedia device in an MMS message.

Claim 12: A method according to claim 1 and further comprising delivering said firstly transcoded content to said first multimedia device, in an MMS message, together with any of said content IDs.

Claim 13: A method according to claim 11 and further comprising:

receiving said firstly transcoded content from said first multimedia device in an MMS message; and

regenerating said content ID of said firstly transcoded content.

Claim 14: A method according to claim 13 wherein said regenerating step comprises regenerating said content ID of said firstly transcoded content using the same method used to generate said content ID of said firstly transcoded content.

Claim 17: A method according to claim 1 and further comprising protecting any of said transcoded content with a content protection key (CPK).

Claim 18: A method according to claim 1 and further comprising:

identifying any rights associated with providing said content to any of said multimedia devices;

generating at least one entitlement as a function of said rights; and

providing said content to any of said multimedia devices in accordance with said entitlement.

Claim 19: A method according to claim 1 and further comprising:

determining if said copy of said firstly transcoded content is protected;

if said copy is protected, determining if said content may be forwarded to said second multimedia device as indicated by any rights associated with either of said content and the recipient of said firstly transcoded content; and

if said content may be forwarded, protecting and forwarding said secondly transcoded content to said second multimedia device.

Claim 20: A method according to claim 19 and further comprising protecting said secondly transcoded content with a content protection key (CPK) associated with said secondly transcoded content.

Claim 21: A method according to claim 19 wherein said first determining step comprises determining that said copy of said firstly transcoded content is protected by identifying a CPK stored in association with the content ID.

Claim 26: A multimedia content distribution system comprising:

an MMS server;

an MMS relay;

a transcoder; and

a DRM server,

wherein at least one of a group consisting of said MMS server, MMS relay, transcoder, and DRM server, is implemented at least partially in hardware;

wherein said MMS server, MMS relay, transcoder, and DRM server are individually or cooperatively operative to:

store an item of a multimedia content as stored multimedia content;

firstly transcode said multimedia content for playback on a first multimedia device, thereby producing a firstly transcoded version of said multimedia content;

generate a content ID of said firstly transcoded version of said multimedia content;

store said content ID of said firstly transcoded version of said multimedia content, as a stored first content ID, in association with said stored multimedia content;

receive an instruction, via a multimedia message service (MMS) message, to forward said item of multimedia content to a second multimedia device, said instruction comprising a copy of said firstly transcoded version of said multimedia content; and

perform the following in response to said instruction:

access said stored content using said stored first content ID of said firstly transcoded version of said multimedia content, comprising:

generating a received content ID of said copy of said firstly transcoded version of said multimedia content; and

looking up said stored multimedia content by comparing said received content ID with said stored first content ID; and

transcode said stored multimedia content for playback on said second multimedia device.

Claim 27: A system according to claim 26 wherein any of said MMS server, MMS relay, transcoder, and DRM server are individually or cooperatively operative to track to whom said content is sent and with what rights.

Claim 28: A system according to claim 26 wherein said DRM server acts as either of a probe and a proxy between any of said MMS server, said MMS relay, and said transcoder.

Claim 29: A system for distributing multimedia content, the system comprising:

means for storing an item of a multimedia content as stored multimedia content at a multimedia message center (MMSC);

means for firstly transcoding said multimedia content for playback on a first multimedia device, thereby producing a firstly transcoded version of said multimedia content;

means for generating a content ID of said firstly transcoded version of said multimedia content;

means for storing said content ID of said firstly transcoded version of said multimedia content, as a stored first content ID, in association with said stored multimedia content;

means for receiving, at said MMSC via a multimedia message service (MMS) message, an instruction to forward said item of multimedia content to a second multimedia device, said instruction comprising a copy of said firstly transcoded version of said multimedia content; and

means for performing the following in response to said instruction:

accessing said stored content using said stored first content ID of said firstly transcoded version of said multimedia content, said accessing comprising:

generating a received content ID of said copy of said firstly transcoded version of said multimedia content; and

looking up said stored multimedia content by comparing said received content ID with said stored first content ID; and

means for transcoding said stored multimedia content for playback on said second multimedia device.

Claim 31: A system according to claim 29 wherein said means for storing is operative to store said item of multimedia content together with an original content identifier (ID) identifying said content.

Claim 32: A system according to claim 29 wherein said means for storing is operative to store said item of multimedia content together with an original content identifier (ID) that uniquely identifies said content.

Claim 33: A system according to claim 29 wherein said means for storing is operative to store said item of multimedia content in its original form.

Claim 34: A system according to claim 29 wherein said means for storing is operative to store said item of multimedia content such that said content may be partly or wholly reconstituted.

Claim 35: A system according to claim 31 and further comprising means for receiving said original content ID from a provider of said content.

Claim 36: A system according to claim 31 and further comprising means for generating said original content ID by applying either of a predefined hashing system and a predefined fingerprinting system to said content and using either of the resulting hash and fingerprint as said original content ID.

Claim 37: A system according to claim 29 and further comprising means for associating said original content ID with different transcoded versions of said content.

Claim 38: A system according to claim 29 and further comprising means for sending a notification to said first multimedia device indicating that said content is available for download to said multimedia device.

Claim 39: A system according to claim 29 and further comprising means for delivering said firstly transcoded content to said first multimedia device in an MMS message.

Claim 40: A system according to claim 29 and further comprising means for delivering said firstly transcoded content to said first multimedia device, in an MMS message, together with any of said content IDs.

Claim 41: A system according to claim 39 and further comprising:

means for receiving said firstly transcoded content from said first multimedia device in an MMS message; and

means for regenerating said content ID of said firstly transcoded content.

Claim 42: A system according to claim 41 wherein said means for regenerating is operative to regenerate said content ID of said firstly transcoded content using the same system used to generate said content ID of said firstly transcoded content.

Claim 45: A system according to claim 29 and further comprising means for protecting any of said transcoded content with a content protection key (CPK).

Claim 46: A system according to claim 29 and further comprising:

means for identifying any rights associated with providing said content to any of said multimedia devices;

means for generating at least one entitlement as a function of said rights; and

means for providing said content to any of said multimedia devices in accordance with said entitlement.

Claim 47: A system according to claim 29 and further comprising:

means for determining if said copy of said firstly transcoded content is protected;

means, responsive to said copy being protected, for determining if said content may be forwarded to said second multimedia device as indicated by any rights associated with either of said content and the recipient of said firstly transcoded content; and

means, responsive to said content being forwardable, for protecting and forwarding said secondly transcoded content to said second multimedia device.

Claim 48: A system according to claim 47 and further comprising means for protecting said secondly transcoded content with a content protection key (CPK) associated with said secondly transcoded content.

Claim 49: A system according to claim 47 wherein said first means for determining is operative to determine that said copy of said firstly transcoded content is protected by identifying a CPK stored in association with the content ID.

Claim 58: A method according to claim 1 and wherein said generating a content ID of said firstly transcoded version of said multimedia content comprises:

applying either of the following to said firstly transcoded version of said multimedia content, and producing a result:

a predefined hashing method; and

a predefined fingerprinting method; and

using said result as said content ID.

Claim 59: A method according to claim 1 and wherein said generating a received content ID of said copy of said firstly transcoded version of said multimedia content comprises:

applying either of the following to said copy of said firstly transcoded version of said multimedia content, and producing a result:

a predefined hashing method; and

a predefined fingerprinting method; and

using said result as said received content ID.

Claim 60: A method according to claim 58 and wherein said generating a received content ID of said copy of said firstly transcoded version of said multimedia content comprises:

applying either of the following to said copy of said firstly transcoded version of said multimedia content, and producing a result:

a predefined hashing method; and

a predefined fingerprinting method; and

using said result as said received content ID.

EVIDENCE APPENDIX

1 Application as filed

2 20 May 2010 Final Office Action

3 29 July 2010 Advisory Action

4 Warst (US 2004/0181550)

5 Malik (US 7,003,551)

OPTIMALLY ADAPTING MULTIMEDIA CONTENT FOR MOBILE SUBSCRIBER DEVICE PLAYBACK

CROSS REFERENCES TO RELATED APPLICATIONS

The present application claims priority from U.S. Provisional Patent Application Number 60/555,717 to Solow et al, filed on March 23, 2004, and U.S. Provisional Patent Application Number 60/635,719 to Solow et al, filed on December 13, 2004, both incorporated herein by reference in their entirety.

FIELD OF THE INVENTION

The present invention relates to communications systems in general, and more particularly to techniques for adapting multimedia content for playback on mobile subscriber devices.

BACKGROUND OF THE INVENTION

The Multimedia Message Service (MMS) provides for the transmission of graphics, video clips, sound files and text messages over wireless networks. Mobile network operators (MNO) and wireless service providers typically implement MMS using MMS Centers (MMSCs), which implement store-and-forward delivery of multimedia messages from providers of multimedia content to mobile subscribers, as well as multimedia message exchange between mobile subscribers. Once a multimedia message is received the MMSC will identify one or more intended recipients of the multimedia message, locate the receiving device of a recipient, which may be a cellular telephone, a PDA or handheld computer, transcode the multimedia message as required for playback on the recipient's device according to the device's multimedia capabilities, and send the multimedia message to the recipient's device.

One challenge facing MNOs and wireless service providers involves adapting multimedia content for the wide variety of mobile subscriber devices in use. Adapting content currently incurs a relatively large computational expense when transcoding content for different playback environments. This is especially acute with respect to multimedia messages sent between disparate mobile subscriber devices. For example, when content

that was previously transcoded for playback on one mobile subscriber device is sent from the mobile subscriber device to another mobile subscriber device, the transcoded content is typically transcoded again by the MMSC for playback on the intended recipient's device. This typically results in a lower playback quality than would be the case if the original content was transcoded for playback on the intended recipient's device. In order for the content to be sent from the mobile subscriber device to another mobile subscriber device of a different type, the transcoded data is typically transcoded again to suit the receiving device, often resulting in a further reduction in quality. Adapting content is further hampered by the complexity of implementing Digital Rights Management (DRM) techniques to control access to content by mobile subscriber devices with different DRM capabilities at a time when DRM standards for MMS are still emerging. Techniques which efficiently adapt multimedia content in these respects would therefore be advantageous.

Furthermore, with current systems, in order to provide control over content each mobile subscriber needs to connect to a content server and download the content in a "pull" mode. A system that would allow mobile subscribers to send content to each other that appears to the recipient as if the content were received in a "push" mode, and that allows for rights management for multimedia devices with different DRM capabilities would also be advantageous.

SUMMARY OF THE INVENTION

In one aspect of the present invention a method is provided for distributing multimedia content, the method including a) storing an item of a multimedia content, b) firstly transcoding the content for playback on a first multimedia device, c) generating a content ID of the firstly transcoded content, d) storing the content ID of the firstly transcoded content in association with the stored content, e) accessing the stored content using the content ID of the firstly transcoded content, and f) secondly transcoding the stored content for playback on a second multimedia device.

In another aspect of the present invention the storing step includes storing the item of multimedia content at a multimedia message center (MMSC).

In another aspect of the present invention the storing step includes storing the item of multimedia content together with an original content identifier (ID) identifying the content.

In another aspect of the present invention the storing step includes storing the item of multimedia content together with an original content identifier (ID) that uniquely identifies the content.

In another aspect of the present invention the storing step includes storing the item of multimedia content in its original form.

In another aspect of the present invention the storing step includes storing the item of multimedia content such that the content may be partly or wholly reconstituted.

In another aspect of the present invention the method further includes receiving the original content ID from a provider of the content.

In another aspect of the present invention the method further includes generating the original content ID by applying either of a predefined hashing method and a predefined fingerprinting method to the content and using either of the resulting hash and fingerprint as the original content ID.

In another aspect of the present invention the method further includes associating the original content ID with different transcoded versions of the content.

In another aspect of the present invention the method further includes sending a notification to the first multimedia device indicating that the content is available for download to the multimedia device.

In another aspect of the present invention the method further includes delivering the firstly transcoded content to the first multimedia device.

In another aspect of the present invention the method further includes delivering the firstly transcoded content to the first multimedia device together with any of the content IDs.

In another aspect of the present invention the method further includes g) receiving the firstly transcoded content from the first multimedia device, and h) regenerating the content ID of the firstly transcoded content.

In another aspect of the present invention the regenerating step includes regenerating the content ID of the firstly transcoded content using the same method used to generate the content ID of the firstly transcoded content.

In another aspect of the present invention the method further includes performing steps e) – h) in response to receiving instructions from the first multimedia device to forward the content to the second multimedia device.

In another aspect of the present invention the performing step includes performing where the instructions include any of a copy of the firstly transcoded content and any of the content IDs.

In another aspect of the present invention the method further includes protecting any of the transcoded content with a content protection key (CPK).

In another aspect of the present invention the method further includes identifying any rights associated with providing the content to any of the multimedia devices, generating at least one entitlement as a function of the rights, and providing the content to any of the multimedia devices in accordance with the entitlement.

In another aspect of the present invention the method further includes determining if the copy of the firstly transcoded content is protected, if the copy is protected, determining if the content may be forwarded to the second multimedia device as indicated by any rights associated with either of the content and the recipient of the firstly transcoded content, and if the content may be forwarded, protecting and forwarding the secondly transcoded content to the second multimedia device.

In another aspect of the present invention the method further includes protecting the secondly transcoded content with a content protection key (CPK) associated with the secondly transcoded content.

In another aspect of the present invention the first determining step includes determining that the copy of the firstly transcoded content is protected by identifying a CPK stored in association with the content ID.

In another aspect of the present invention a method is provided for implementing digital rights management (DRM), the method including determining the DRM capabilities of a multimedia device, determining the DRM rights associated with an item of content, determining an optimal level of DRM protection to apply to the content as

a function of the capabilities and the rights, and applying the optimal level of DRM protection to the item of content.

In another aspect of the present invention the determining an optimal level step includes determining the optimal level as the highest-ranked level of DRM protection that is both supported by the device and that is indicated by the content rights.

In another aspect of the present invention the determining an optimal level step includes determining the optimal level as the highest-ranked level of DRM protection that is supported by the device.

In another aspect of the present invention the determining an optimal level step includes determining the optimal level as the highest-ranked level of DRM protection that is that is indicated by the content rights and that is below the highest-ranked level of DRM protection that is that is supported by the device.

In another aspect of the present invention a multimedia content distribution system is provided including an MMS server, an MMS relay, a transcoder, and a DRM server, where the MMS server, MMS relay, transcoder, and DRM server are individually or cooperatively operative to store an item of a multimedia content, firstly transcode the content for playback on a first multimedia device, generate a content ID of the firstly transcoded content, store the content ID of the firstly transcoded content in association with the stored content, access the stored content using the content ID of the firstly transcoded content, and secondly transcode the stored content for playback on a second multimedia device.

In another aspect of the present invention any of the MMS server, MMS relay, transcoder, and DRM server are individually or cooperatively operative to track to whom the content is sent and with what rights.

In another aspect of the present invention the DRM server acts as either of a probe and a proxy between any of the MMS server, the MMS relay, and the transcoder.

In another aspect of the present invention a system is provided for distributing multimedia content, the system including a) means for storing an item of a multimedia content, b) means for firstly transcoding the content for playback on a first multimedia device, c) means for generating a content ID of the firstly transcoded content, d) means for storing the content ID of the firstly transcoded content in association with the stored

content, e) means for accessing the stored content using the content ID of the firstly transcoded content, and f) means for secondly transcoding the stored content for playback on a second multimedia device.

In another aspect of the present invention the means for storing is operative to store the item of multimedia content at a multimedia message center (MMSC).

In another aspect of the present invention the means for storing is operative to store the item of multimedia content together with an original content identifier (ID) identifying the content.

In another aspect of the present invention the means for storing is operative to store the item of multimedia content together with an original content identifier (ID) that uniquely identifies the content.

In another aspect of the present invention the means for storing is operative to store the item of multimedia content in its original form.

In another aspect of the present invention the means for storing is operative to store the item of multimedia content such that the content may be partly or wholly reconstituted.

In another aspect of the present invention the system further includes means for receiving the original content ID from a provider of the content.

In another aspect of the present invention the system further includes means for generating the original content ID by applying either of a predefined hashing system and a predefined fingerprinting system to the content and using either of the resulting hash and fingerprint as the original content ID.

In another aspect of the present invention the system further includes means for associating the original content ID with different transcoded versions of the content.

In another aspect of the present invention the system further includes means for sending a notification to the first multimedia device indicating that the content is available for download to the multimedia device.

In another aspect of the present invention the system further includes means for delivering the firstly transcoded content to the first multimedia device.

In another aspect of the present invention the system further includes means for delivering the firstly transcoded content to the first multimedia device together with any. of the content IDs.

In another aspect of the present invention the system further includes g) means for receiving the firstly transcoded content from the first multimedia device, and h) means for regenerating the content ID of the firstly transcoded content.

In another aspect of the present invention the means for regenerating is operative to regenerate the content ID of the firstly transcoded content using the same system used to generate the content ID of the firstly transcoded content.

In another aspect of the present invention the means e) – h) are operative in response to receiving instructions from the first multimedia device to forward the content to the second multimedia device.

In another aspect of the present invention the instructions include any of a copy of the firstly transcoded content and any of the content IDs.

In another aspect of the present invention the system further includes means for protecting any of the transcoded content with a content protection key (CPK).

In another aspect of the present invention the system further includes means for identifying any rights associated with providing the content to any of the multimedia devices, means for generating at least one entitlement as a function of the rights, and means for providing the content to any of the multimedia devices in accordance with the entitlement.

In another aspect of the present invention the system further includes means for determining if the copy of the firstly transcoded content is protected, means, responsive to the copy being protected, for determining if the content may be forwarded to the second multimedia device as indicated by any rights associated with either of the content and the recipient of the firstly transcoded content, and means, responsive to the content being forwardable, for protecting and forwarding the secondly transcoded content to the second multimedia device.

In another aspect of the present invention the system further includes means for protecting the secondly transcoded content with a content protection key (CPK) associated with the secondly transcoded content.

In another aspect of the present invention the first means for determining is operative to determine that the copy of the firstly transcoded content is protected by identifying a CPK stored in association with the content ID.

In another aspect of the present invention a system is provided for implementing digital rights management (DRM), the system including means for determining the DRM capabilities of a multimedia device, means for determining the DRM rights associated with an item of content, means for determining an optimal level of DRM protection to apply to the content as a function of the capabilities and the rights, and means for applying the optimal level of DRM protection to the item of content.

In another aspect of the present invention the means for determining an optimal level is operative to determine the optimal level as the highest-ranked level of DRM protection that is both supported by the device and that is indicated by the content rights.

In another aspect of the present invention the means for determining an optimal level is operative to determine the optimal level as the highest-ranked level of DRM protection that is supported by the device.

In another aspect of the present invention the means for determining an optimal level is operative to determine the optimal level as the highest-ranked level of DRM protection that is that is indicated by the content rights and that is below the highest-ranked level of DRM protection that is that is supported by the device.

It is appreciated throughout the specification and claims that the term "multimedia" as it applies to content may include audio content, visual content including text, still images, and/or moving images, and any combination thereof.

BRIEF DESCRIPTION OF THE DRAWINGS

The present invention will be understood and appreciated more fully from the following detailed description taken in conjunction with the appended drawings in which:

Figs. 1A and 1B, which are simplified block-flow diagrams of a multimedia content distribution system for non-encrypted content, constructed and operative in accordance with a preferred embodiment of the present invention;

Figs. 1C and 1D, which are simplified block-flow diagrams of a multimedia content distribution system for encrypted content, constructed and operative in accordance with a preferred embodiment of the present invention;

Fig. 2 is a simplified block diagram of a multimedia service center, constructed and operative in accordance with a preferred embodiment of the present invention;

Fig. 3 is a simplified block diagram of a multimedia service center, constructed and operative in accordance with a preferred embodiment of the present invention; and

Fig. 4 is a simplified flowchart illustration of a method for implementing best effort DRM, operative in accordance with a preferred embodiment of the present invention.

The same reference characters and numerals appearing on different drawings denote the same elements.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

Reference is now made to Figs. 1A and 1B, which are simplified block-flow diagrams of a multimedia content distribution system for non-encrypted content, constructed and operative in accordance with a preferred embodiment of the present invention. In Fig. 1A a multimedia content provider 100 is shown providing multimedia content to a multimedia message center (MMSC) 102, for delivery to a multimedia device, such as a cellular telephone, of a mobile subscriber 104, labeled 'A'. Preferred implementations of MMSC 102 are described in greater detail hereinbelow with reference to Figs. 2 and 3. After receiving the content, MMSC 102 preferably stores the content in a database 106, either in its original form or otherwise such that the original content may be partly or wholly reconstituted. The content is preferably stored along with an original content identifier (ID) that preferably uniquely identifies the content. The original content ID may be received from multimedia content provider 100 or may be generated for the content using any suitable technique. For example, the original content ID may be generated by applying a predefined hashing or fingerprinting method to the content and using the resulting hash or fingerprint as the original content ID. The same original content ID associated with the original content received from multimedia content provider 100 may be associated with different transcoded versions of the content as may be prepared for playback by different multimedia devices. Alternatively, a different content ID may be

generated by applying a predefined hashing or fingerprinting method to each transcoded version of the content and using the resulting hash or fingerprint as the content ID for its associated transcoded version. In this scenario, the content ID of each transcoded version is preferably stored by MMSC 102 in database 106 together with the original content and/or the original content ID of the original content.

Once the content is received from multimedia content provider 100, MMSC 102 preferably sends a notification to the multimedia device of mobile subscriber A indicating that content intended for subscriber A is available for download from MMSC 102. When mobile subscriber A contacts MMSC 102 to retrieve the content, or in anticipation of such contact, MMSC 102 may transcode the content as necessary for playback on his/her multimedia device whose characteristics may be determined by MMSC 102 using conventional techniques. A content ID of the content transcoded for mobile subscriber A may then preferably generated as described above and stored in database 106 in association with the original content. The content transcoded for mobile subscriber A is then delivered to mobile subscriber A using conventional techniques. The transcoded content may be transmitted to mobile subscriber A together with the original content ID associated with the original content, which may be transmitted "in the clear" or unencrypted, and/or together with the content ID generated for the transcoded content.

It will be appreciated that once a content ID is generated by MMSC 102 for a specific content item that has been transcoded for a particular type of recipient multimedia device, a content ID need not be generated again for the transcoded content adapted for the same type of device as long as the content ID is retained by MMSC 102. The transcoded content may itself optionally be stored in database 106, such as in anticipation of the transcoded content being provided to other mobile devices for which the transcoded content is adapted for playback.

In the system of Fig. 1B MMSC 102 is shown receiving from mobile subscriber A instructions to forward content previously provided to mobile subscriber A to the multimedia device of a mobile subscriber 108, labeled 'B'. The instructions may include a copy of the transcoded content previously provided to mobile subscriber A, the original content ID associated with the original content, and/or the content ID generated for the transcoded content. After receiving the instructions from mobile subscriber A, MMSC

102 preferably sends a notification to the multimedia device of mobile subscriber B indicating that content intended for subscriber B is available for download from MMSC 102. When mobile subscriber B contacts MMSC 102 to retrieve the content, or in anticipation of such contact, if a content ID associated with the content is received from mobile subscriber A, such as a part of submitted content data, MMSC 102 may determine the original content by looking up the content ID in database 106. If no content ID is received from mobile subscriber A, MMSC 102 preferably regenerates a content ID of the received content using the same method used to created the content ID when previously transcoding the content for mobile subscriber A. MMSC 102 then looks up the regenerated content ID in database 106 to identify the original content associated with the content ID. Once found, the original content is retrieved and transcoded as necessary for playback on the multimedia device of mobile subscriber B whose characteristics may be determined by MMSC 102 using conventional techniques. As before, a content ID of the content transcoded for mobile subscriber B may be generated using any suitable method, preferably being the same method previously used to generate a content ID for the content transcoded for mobile subscriber A. The content ID is then preferably stored in database 106 in association with the original content. The content transcoded for mobile subscriber B is then delivered to mobile subscriber B using conventional techniques.

Reference is now made to Figs. 1C and 1D, which are simplified block-flow diagrams of a multimedia content distribution system for encrypted content, constructed and operative in accordance with a preferred embodiment of the present invention. The system of Fig. 1C is similar to the system of Fig. 1A except as is now noted. In the system of Fig. 1C MMSC 102 stores content access criteria (e.g. "forward lock") in database 106 in association with the original content, where the content access criteria may be specified and provided by multimedia content provider 100 or the service provider (e.g. a MNO). MMSC 102 preferably generates a Content Protection Key (CPK) using conventional key generation techniques and stores the CPK in database 106 in association with the content. The CPK may be generated once for a content item and may be reused for various mobile subscriber devices. Alternatively, a unique CPK may be generated for different mobile subscriber devices and even for different transactions involving the same mobile subscriber device. After the content is transcoded for mobile subscriber A, MMSC 102 preferably

protects the transcoded content using the CPK, such as by employing an encryption method such as AES. MMSC 102 preferably identifies any rights associated with providing content to mobile subscriber A, such as by evaluating the content access criteria associated with the content, as well as any rights associated with mobile subscriber A in accordance with conventional rights assessment techniques. MMSC 102 then preferably generates and stores in database 106 subscribe any entitlements associated with the content, such as whether mobile subscriber A has the right to receive the content. A content ID of the content that has been transcoded and protected for mobile subscriber A may then be generated as described above and stored in database 106 in association with the original content. The transcoded and protected content is then delivered to mobile subscriber A using conventional techniques.

The system of Fig. 1D is similar to the system of Fig. 1B except as is now noted. In the system of Fig. 1D when MMSC 102 receives from mobile subscriber A instructions to send content previously provided to mobile subscriber A to the multimedia device of mobile subscriber B, MMSC 102 receives a content ID of the received content, or generates a content ID of the received content as described above, and then looks up the content ID in database 106 to determine if the received content is protected, such as may be evidenced by the presence of a CPK stored in association with the content ID. If the received content is protected, MMSC 102 preferably identifies the content access criteria, specified by the content or service provider associated with the received content item and then verifies the rights of A, determining if mobile subscriber A is allowed to forward the content to mobile subscriber B. If the content rights do not allow the content to be forwarded, the transaction ends. If the content rights allow the content to be forwarded, MMSC 102 sends a notification to mobile subscriber B indicating that content intended for subscriber B is available for download from MMSC 102. When mobile subscriber B contacts MMSC 102 to retrieve the content, or in anticipation of such contact, MMSC 102 retrieves the original content from database 106 using the content ID. The original content is transcoded according to the multimedia device capabilities of mobile subscriber B. MMSC 102 preferably generates and stores a CPK for mobile subscriber B. Alternatively, MMSC 102 may use the same CPK previously generated for the content item. MMSC 102 protects the transcoded content with the CPK, such as by encrypting the transcoded

content with AES. A content ID of the content transcoded and protected for mobile subscriber B is then preferably generated as described above and stored in database 106 in association with the original content. The content transcoded for mobile subscriber B is then delivered to mobile subscriber B using conventional techniques.

Reference is now made to Fig. 2, which is a simplified block diagram of a multimedia service center, constructed and operative in accordance with a preferred embodiment of the present invention. In Fig. 2 an MMSC 200 is shown having an MMS server 202 which controls the storage aspect of the store-and-forward MMS architecture, and an MMS relay 204 which controls transcoding and delivery of multimedia messages to mobile subscribers. Also shown in Fig. 2 are additional MMS architecture elements, any of which may be incorporated into MMSC 200 or provided externally to MMSC 200 with which MMSC 200 may communicate. These elements may include an MMS user agent 206, that provides users with the ability to view, create, send, edit, delete and manage their multimedia messages, a transcoder 208 for transcoding multimedia content as may be required for playback on mobile subscriber devices, a DRM server 210 for providing digital rights management of content, a billing system 212 for billing subscribers, an MMS value added service (VAS) application 214 for providing multimedia content, such as weather reports and music video clips, an MMS user database 216 for storing subscriber information, a home location register (HLR) 218 which provides subscriber routing information and maintenance of user subscription information, and one or more external servers 220 for providing auxiliary services such as faxing, email, and unified messaging service (UMS). Communications between elements shown in Fig. 2 may be performed in accordance with conventional protocols, such as multimedia protocols MM1 – MM9 and DRM protocols as shown.

Any of the functions described hereinabove with reference to Figs. 1A – 1E may be performed by any of the elements shown in Fig. 2, or cooperatively by any combination of any of the elements shown in Fig. 2, such as by DRM server 210 in addition to performing digital rights management operations to protect content. DRM server 210 may perform content ID generation at any stage before or after transcoding and/or protecting content. DRM server 210 and/or any of the elements shown in Fig. 2

may also track to whom content is sent and with what rights, which, for example, may be used to generate a log for a content provider.

Reference is now made to Fig. 3, which is a simplified block diagram of a multimedia service center, constructed and operative in accordance with a preferred embodiment of the present invention. Figs. 2 and 3 are substantially similar, with the notable exception that in Fig. 3 DRM server 210 does not interface directly with MMSC 200. Rather, DRM server 210 acts as a probe and/or proxy between MMSC 200 and other elements described in Fig. 2.

Reference is now made to Fig. 4, which is a simplified flowchart illustration of a method for implementing DRM, operative in accordance with a preferred embodiment of the present invention. In the method of Fig. 4, which may be implemented by DRM server 210 of Figs. 2 and 3 separate from or in addition to the functions described hereinabove with reference to Figs. 1A – 1E, MMSC 200 receives content for distribution to a mobile subscriber. DRM Server 210 determines the DRM capabilities of the mobile subscriber device using conventional techniques, such as by receiving information about the device from MMSC 200, which may receive such information from the device itself or from device information previously stored in database 216, and consulting a table of DRM capabilities by device or a User Agent Profile (UAProf) of the device acquired using conventional techniques. Such DRM capabilities may be built in to the device, or may be programmed into the device after manufacture, such as by loading a multimedia player client with DRM capabilities into the device. DRM Server 210 also determines the "content rights" indicating what type of DRM protection applies to the content itself, such as may be indicated by the content provider and/or the service provider. Given the above information DRM Server 210 determines an optimal level of DRM protection to apply to the content as a function of said device DRM capabilities and content rights, such as may be based on a predefined ranking of levels of DRM protection. Thus, in one possible configuration, the highest-ranked level of DRM protection that is both supported by the mobile subscriber device and that is indicated by the content rights may be selected and applied to the content. In another possible configuration, if the content provider and/or the wireless service provider require a level of DRM protection that is ranked below the highest level of protection that is supported by the mobile subscriber device, DRM server

210 may select and apply the level of DRM protection required by the content provider and/or the wireless service provider. In another possible configuration, if the maximum level of DRM protection that is supported by the mobile subscriber device is ranked below a minimum level of DRM protection required by the content provider and/or the wireless service provider, the content may be withheld from the mobile subscriber device. Alternatively, DRM server 210 may provide the mobile subscriber device with software to support either the maximum level of DRM protection that can be supported by the mobile subscriber device using such software or the maximum level of DRM protection required by the content provider and/or the wireless service provider.

The method of Fig. 4 may be used to implement a DRM rights hierarchy, such as is provided by the OMA-1 standard, where different rights modes are represented from strongest to weakest as follows:

SD - separate delivery

CD - combined delivery

FL - forward lock

Clear – "in the clear"

Thus, for example, if these rights are associated with an item of content, delivery of the content to a multimedia device will first be attempted by implementing SD, provided that the multimedia device supports SD. If the multimedia device does not support SD, delivery of the content will then be attempted by implementing CD, and so forth.

Another example of a DRM rights hierarchy may be understood where a device supports two or more different DRM systems, each one with own method of content protection and rights management. For instance, where a device is configured by its manufacturer to support the OMA DRM v1 implementation, and is also equipped with a third-party proprietary DRM system which uses a proven-key management scheme involving secure hardware (e.g. a SIM or other chip in the device platform), the DRM server may chose to protect content using the third-party proprietary DRM format, where the server includes a ranking of the third-party proprietary DRM system with respect to OMA DRM v1 and determines that the third-party DRM provides better security then OMA DRM v1.

The method of Fig. 4 may be understood in the context the following example, where a content provider agrees to provide some video clips to a content aggregator. The content provider stipulates that the strongest OMA-1 rights protection be implemented, that content not be sent in the clear, and that it is willing to receive a payment from the content aggregator for any clip received by a mobile subscriber. The content aggregator has an MMSC connected to a DRM Server as described above. A mobile subscriber, Joe, has a multimedia device which implements OMA-1 forward lock functionality only. The DRM Server analyses the information and makes a decision to protect content as an OMA-1 forward-lock DRM message, since this is the only DRM option available for this user.

Another user, Alice, has a multimedia device which implements the full OMA-1 standard. When Alice retrieves a clip, the DRM Server makes a decision to protect content according to OMA-1 Separate Delivery method. This method may be preferred by the DRM Server because a) it is much more secure, since the content is encrypted, and b) Alice will be able to share content with her friends, while the content is still protected and each new recipient will be required to acquire his/her own rights to access the content

Another user, Michael, has a multimedia device that is able to play content provided by the content provider, but has no DRM capabilities. The content aggregator uses the DRM Server to identify users that can receive protected content and thus does not send an announcement to Michael that the content is available. However, Alice forwarded the announcement she received to Michael. When Michael tries to retrieve a clip, the DRM Server informs the MMSC that content can not be protected for Michael's device. Alice may receive a message that Michael cannot receive the forwarded content, and/or Michael may receive a message saying that content that Alice wished to forward can not be released for his device.

Another user, Leo, has a multimedia device with some DRM capabilities provided by the device manufacturer. Additionally, Leo has registered at the content aggregator's WAP site for a premium content service called "Video Hit of The Day." The content aggregator asks Leo to download and install a third-party DRM agent on his device. When Leo attempts to access content, the DRM Server checks its database and finds that Leo has installed a third-party DRM Agent, with this information being recorded by the content aggregator when Leo downloaded the DRM Agent. The DRM Server

analyses the DRM capabilities both inherent in Leo's device and otherwise installed in Leo's device and decides that maximum protection may be achieved by using the third-party DRM Agent. The DRM Server protects the content according to the maximum protection supported by the third-party DRM Agent.

It is appreciated that one or more of the steps of any of the methods described herein may be omitted or carried out in a different order than that shown, without departing from the true spirit and scope of the invention.

While the methods and apparatus disclosed herein may or may not have been described with reference to specific computer hardware or software, it is appreciated that the methods and apparatus described herein may be readily implemented in computer hardware or software using conventional techniques.

While the present invention has been described with reference to one or more specific embodiments, the description is intended to be illustrative of the invention as a whole and is not to be construed as limiting the invention to the embodiments shown. It is appreciated that various modifications may occur to those skilled in the art that, while not specifically shown herein, are nevertheless within the true spirit and scope of the invention. Various features of the invention which are, for clarity, described in the contexts of separate embodiments may also be provided in combination in a single embodiment. Conversely, various features of the invention which are, for brevity, described in the context of a single embodiment may also be provided separately or in any suitable subcombination.

CLAIMS

What is claimed is:

1. A method for distributing multimedia content, the method comprising:

a) storing an item of a multimedia content;

b) firstly transcoding said content for playback on a first multimedia device;

c) generating a content ID of said firstly transcoded content;

d) storing said content ID of said firstly transcoded content in association with said stored content;

e) accessing said stored content using said content ID of said firstly transcoded content; and

f) secondly transcoding said stored content for playback on a second multimedia device.

2. A method according to claim 1 wherein said storing step comprises storing said item of multimedia content at a multimedia message center (MMSC).

3. A method according to claim 1 wherein said storing step comprises storing said item of multimedia content together with an original content identifier (ID) identifying said content.

4. A method according to claim 1 wherein said storing step comprises storing said item of multimedia content together with an original content identifier (ID) that uniquely identifies said content.

5. A method according to claim 1 wherein said storing step comprises storing said item of multimedia content in its original form.

6. A method according to claim 1 wherein said storing step comprises storing said item of multimedia content such that said content may be partly or wholly reconstituted.

7. A method according to claim 3 and further comprising receiving said original content ID from a provider of said content.

8. A method according to claim 3 and further comprising generating said original content ID by applying either of a predefined hashing method and a predefined fingerprinting method to said content and using either of the resulting hash and fingerprint as said original content ID.

9. A method according to claim 1 and further comprising associating said original content ID with different transcoded versions of said content.

10. A method according to claim 1 and further comprising sending a notification to said first multimedia device indicating that said content is available for download to said multimedia device.

11. A method according to claim 1 and further comprising delivering said firstly transcoded content to said first multimedia device.

12. A method according to claim 1 and further comprising delivering said firstly transcoded content to said first multimedia device together with any of said content IDs.

13. A method according to claim 11 and further comprising:

g) receiving said firstly transcoded content from said first multimedia device; and

h) regenerating said content ID of said firstly transcoded content.

14. A method according to claim 13 wherein said regenerating step comprises regenerating said content ID of said firstly transcoded content using the same method used to generate said content ID of said firstly transcoded content.

15. A method according to claim 13 and further comprising performing steps e) – h) in response to receiving instructions from said first multimedia device to forward said content to said second multimedia device.

16. A method according to claim 15 wherein said performing step comprises performing where said instructions include any of a copy of said firstly transcoded content and any of said content IDs.

17. A method according to claim 1 and further comprising protecting any of said transcoded content with a content protection key (CPK).

18. A method according to claim 1 and further comprising:

identifying any rights associated with providing said content to any of said multimedia devices;

generating at least one entitlement as a function of said rights; and

providing said content to any of said multimedia devices in accordance with said entitlement.

19. A method according to claim 16 and further comprising:

determining if said copy of said firstly transcoded content is protected;

if said copy is protected, determining if said content may be forwarded to said second multimedia device as indicated by any rights associated with either of said content and the recipient of said firstly transcoded content; and

if said content may be forwarded, protecting and forwarding said secondly transcoded content to said second multimedia device.

20. A method according to claim 19 and further comprising protecting said secondly transcoded content with a content protection key (CPK) associated with said secondly transcoded content.

21. A method according to claim 19 wherein said first determining step comprises determining that said copy of said firstly transcoded content is protected by identifying a CPK stored in association with the content ID.

22. A method for implementing digital rights management (DRM), the method comprising:

determining the DRM capabilities of a multimedia device;

determining the DRM rights associated with an item of content;

determining an optimal level of DRM protection to apply to said content as a function of said capabilities and said rights; and

applying said optimal level of DRM protection to said item of content.

23. A method according to claim 22 wherein said determining an optimal level step comprises determining said optimal level as the highest-ranked level of DRM protection that is both supported by said device and that is indicated by said content rights.

24. A method according to claim 22 wherein said determining an optimal level step comprises determining said optimal level as the highest-ranked level of DRM protection that is supported by said device.

25. A method according to claim 22 wherein said determining an optimal level step comprises determining said optimal level as the highest-ranked level of DRM protection that is that is indicated by said content rights and that is below the highest-ranked level of DRM protection that is that is supported by said device.

26. A multimedia content distribution system comprising:

an MMS server;

an MMS relay;

a transcoder; and

a DRM server,

wherein said MMS server, MMS relay, transcoder, and DRM server are individually or cooperatively operative to:

store an item of a multimedia content;

firstly transcode said content for playback on a first multimedia device;

generate a content ID of said firstly transcoded content;

store said content ID of said firstly transcoded content in association with said stored content;

access said stored content using said content ID of said firstly transcoded content; and

secondly transcode said stored content for playback on a second multimedia device.

27. A system according to claim 26 wherein any of said MMS server, MMS relay, transcoder, and DRM server are individually or cooperatively operative to track to whom said content is sent and with what rights.

28. A system according to claim 26 wherein said DRM server acts as either of a probe and a proxy between any of said MMS server, said MMS relay, and said transcoder.

29. A system for distributing multimedia content, the system comprising:

a) means for storing an item of a multimedia content;

b) means for firstly transcoding said content for playback on a first multimedia device;

c) means for generating a content ID of said firstly transcoded content;

d) means for storing said content ID of said firstly transcoded content in association with said stored content;

e) means for accessing said stored content using said content ID of said firstly transcoded content; and

f) means for secondly transcoding said stored content for playback on a second multimedia device.

30. A system according to claim 29 wherein said means for storing is operative to store said item of multimedia content at a multimedia message center (MMSC).

31. A system according to claim 29 wherein said means for storing is operative to store said item of multimedia content together with an original content identifier (ID) identifying said content.

32. A system according to claim 29 wherein said means for storing is operative to store said item of multimedia content together with an original content identifier (ID) that uniquely identifies said content.

33. A system according to claim 29 wherein said means for storing is operative to store said item of multimedia content in its original form.

34. A system according to claim 29 wherein said means for storing is operative to store said item of multimedia content such that said content may be partly or wholly reconstituted.

35. A system according to claim 31 and further comprising means for receiving said original content ID from a provider of said content.

36. A system according to claim 31 and further comprising means for generating said original content ID by applying either of a predefined hashing system and a predefined fingerprinting system to said content and using either of the resulting hash and fingerprint as said original content ID.

37. A system according to claim 29 and further comprising means for associating said original content ID with different transcoded versions of said content.

38. A system according to claim 29 and further comprising means for sending a notification to said first multimedia device indicating that said content is available for download to said multimedia device.

39. A system according to claim 29 and further comprising means for delivering said firstly transcoded content to said first multimedia device.

40. A system according to claim 29 and further comprising means for delivering said firstly transcoded content to said first multimedia device together with any of said content IDs.

41. A system according to claim 39 and further comprising:

g) means for receiving said firstly transcoded content from said first multimedia device; and

h) means for regenerating said content ID of said firstly transcoded content.

42. A system according to claim 41 wherein said means for regenerating is operative to regenerate said content ID of said firstly transcoded content using the same system used to generate said content ID of said firstly transcoded content.

43. A system according to claim 41 where said means e) – h) are operative in response to receiving instructions from said first multimedia device to forward said content to said second multimedia device.

44. A system according to claim 43 wherein said instructions include any of a copy of said firstly transcoded content and any of said content IDs.

45. A system according to claim 29 and further comprising means for protecting any of said transcoded content with a content protection key (CPK).

46. A system according to claim 29 and further comprising:

means for identifying any rights associated with providing said content to any of said multimedia devices;

means for generating at least one entitlement as a function of said rights; and

means for providing said content to any of said multimedia devices in accordance with said entitlement.

47. A system according to claim 44 and further comprising:

means for determining if said copy of said firstly transcoded content is protected;

means, responsive to said copy being protected, for determining if said content may be forwarded to said second multimedia device as indicated by any rights associated with either of said content and the recipient of said firstly transcoded content; and

means, responsive to said content being forwardable, for protecting and forwarding said secondly transcoded content to said second multimedia device.

48. A system according to claim 47 and further comprising means for protecting said secondly transcoded content with a content protection key (CPK) associated with said secondly transcoded content.

49. A system according to claim 47 wherein said first means for determining is operative to determine that said copy of said firstly transcoded content is protected by identifying a CPK stored in association with the content ID.

50. A system for implementing digital rights management (DRM), the system comprising:

means for determining the DRM capabilities of a multimedia device;

means for determining the DRM rights associated with an item of content;

means for determining an optimal level of DRM protection to apply to said content as a function of said capabilities and said rights; and

means for applying said optimal level of DRM protection to said item of content.

51. A system according to claim 50 wherein said means for determining an optimal level is operative to determine said optimal level as the highest-ranked level of DRM

protection that is both supported by said device and that is indicated by said content rights.

52. A system according to claim 50 wherein said means for determining an optimal level is operative to determine said optimal level as the highest-ranked level of DRM protection that is supported by said device.

53. A system according to claim 50 wherein said means for determining an optimal level is operative to determine said optimal level as the highest-ranked level of DRM protection that is that is indicated by said content rights and that is below the highest-ranked level of DRM protection that is that is supported by said device.

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
29 September 2005 (29.09.2005)

PCT

(10) International Publication Number
WO 2005/089061 A2

(51) International Patent Classification: Not classified

(21) International Application Number:
PCT/IL2005/000319

(22) International Filing Date: 21 March 2005 (21.03.2005)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/555,717 23 March 2004 (23.03.2004) US
60/635,719 13 December 2004 (13.12.2004) US

(71) Applicant *(for all designated States except US)*: NDS LIMITED [GB/GB]; One London Road, Staines Middlesex TW18 4EX (GB).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: MAIL, David [IL/IL]; 16 Emek Dotan St., 44862 Zur Igal (IL). SOLOW, Hillel [IL/IL]; 115 Shimon St., 99543 Beit Shemesh (IL). WAISBARD, Erez [IL/IL]; 7 Moshe Dayan St., 60401 Or-Yehuda (IL). SELDIN, Anatoly [IL/IL]; 18/3 Rabbi Meir St., 93185 Jerusalem (IL). BOGOT, Carmi [IL/IL]; 13 Ha-Metzlitayim St., 98420 Maaleh Adumim (IL).

(74) Agent: SWIRSKY, Daniel J.; AlphaPatent Associates Ltd., P.O.B. 2345, 99544 BEIT SHEMESH (IL).

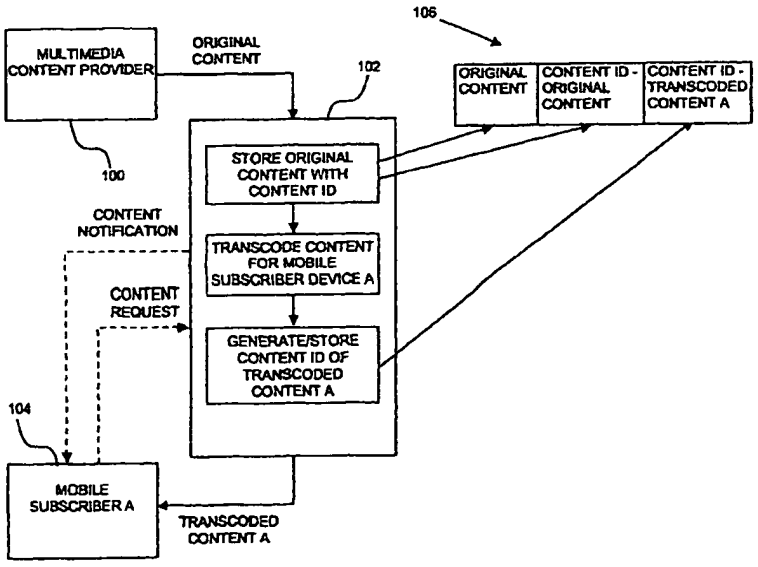
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *without international search report and to be republished upon receipt of that report*

[Continued on next page]

(54) Title: OPTIMALLY ADAPTING MULTIMEDIA CONTENT FOR MOBILE SUBSCRIBER DEVICE PLAYBACK



(57) Abstract: A multimedia content distribution method including a) storing an item of a multimedia content, b) firstly transcoding the content for playback on a first multimedia device, c) generating a content ID of the firstly transcoded content, d) storing the content ID of the firstly transcoded content in association with the stored content, e) accessing the stored content using the content ID of the firstly transcoded content, and f) secondly transcoding the stored content for playback on a second multimedia device.

WO 2005/089061 A2

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

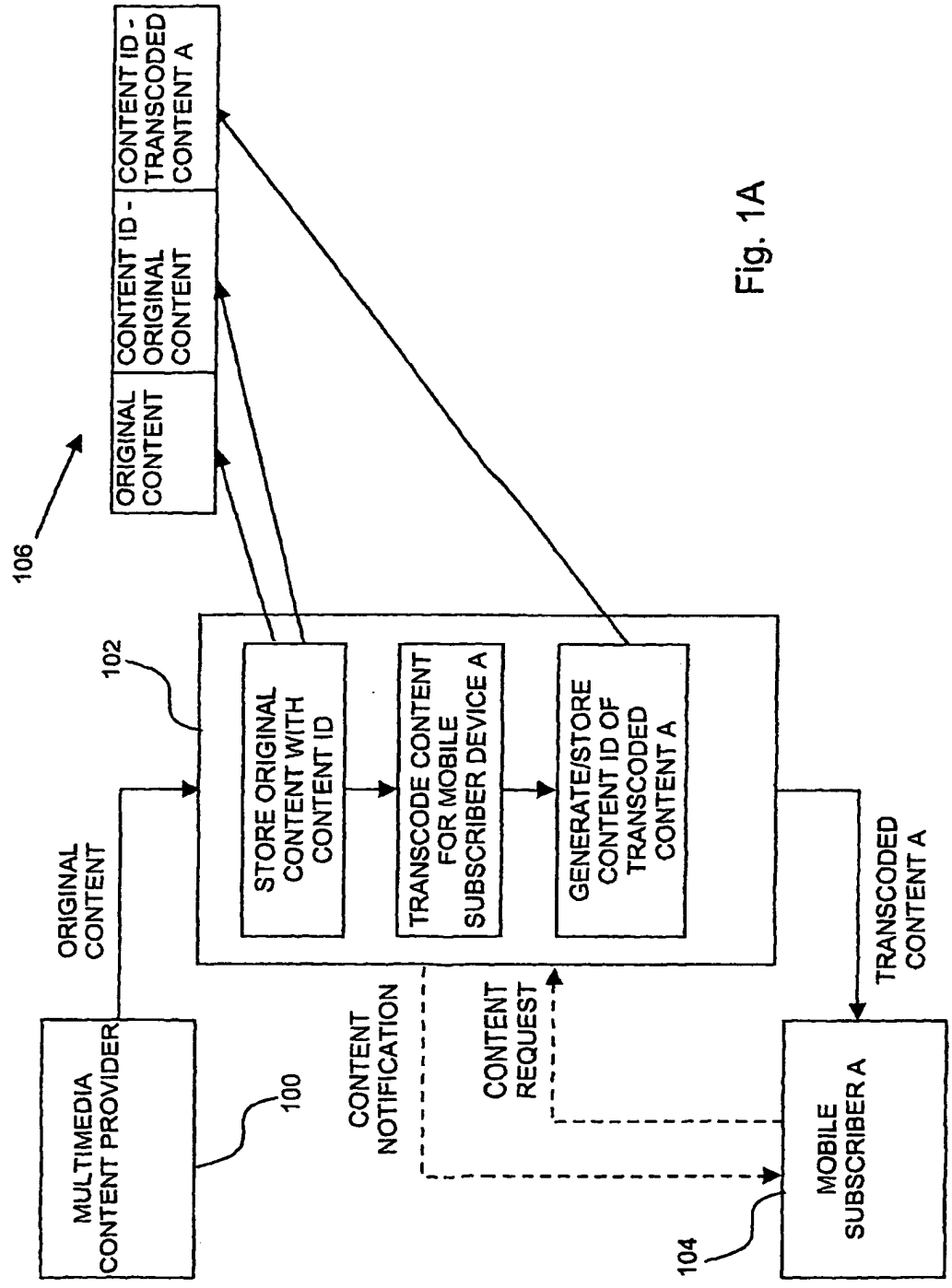

MULTIMEDIA CONTENT PROVIDER
100
ORIGINAL CONTENT
102
STORE ORIGINAL CONTENT WITH CONTENT ID
TRANSCODE CONTENT FOR MOBILE SUBSCRIBER DEVICE A
GENERATE/STORE CONTENT ID OF TRANSCODED CONTENT A
TRANSCODED CONTENT A
CONTENT NOTIFICATION
CONTENT REQUEST
MOBILE SUBSCRIBER A
104
106
ORIGINAL CONTENT
CONTENT ID - ORIGINAL CONTENT
CONTENT ID - TRANSCODED CONTENT A

Fig. 1A

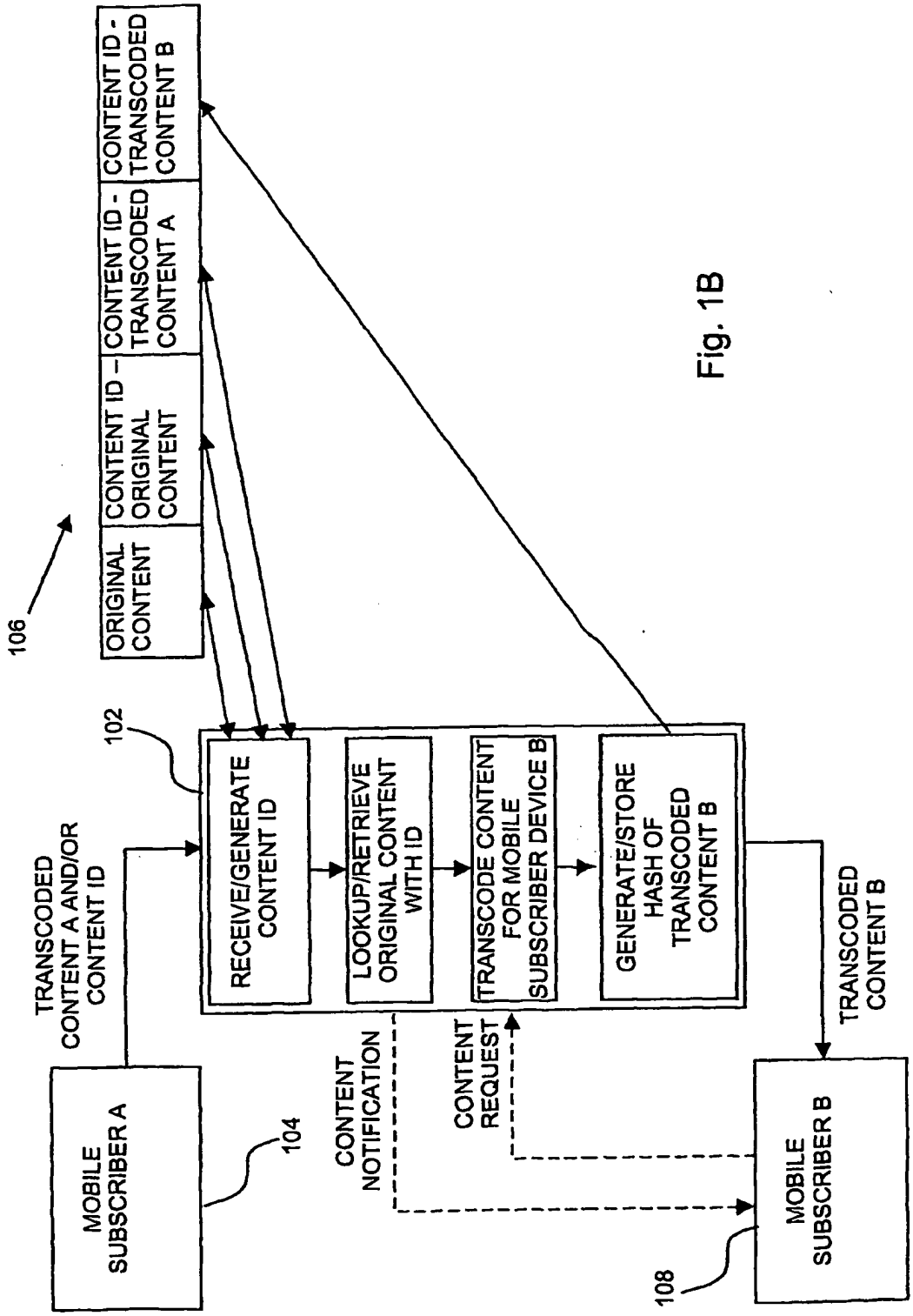

106
ORIGINAL CONTENT
CONTENT ID – ORIGINAL CONTENT
CONTENT ID - TRANSCODED CONTENT A
CONTENT ID - TRANSCODED CONTENT B
102
RECEIVE/GENERATE CONTENT ID
LOOKUP/RETRIEVE ORIGINAL CONTENT WITH ID
TRANSCODE CONTENT FOR MOBILE SUBSCRIBER DEVICE B
GENERATE/STORE HASH OF TRANSCODED CONTENT B
TRANSCODED CONTENT A AND/OR CONTENT ID
MOBILE SUBSCRIBER A
104
CONTENT NOTIFICATION
CONTENT REQUEST
TRANSCODED CONTENT B
MOBILE SUBSCRIBER B
108

Fig. 1B

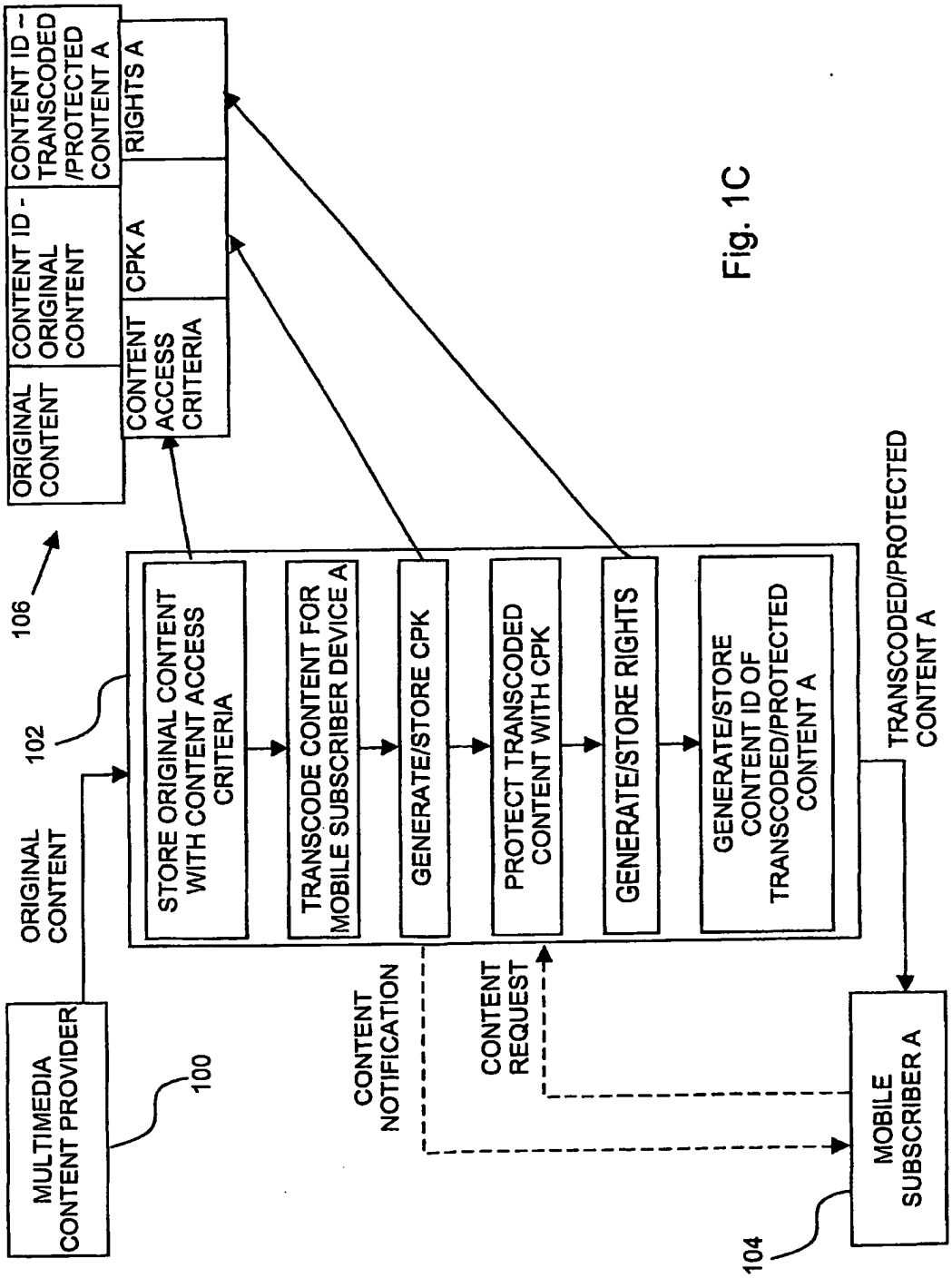

MULTIMEDIA CONTENT PROVIDER
100
ORIGINAL CONTENT
102
STORE ORIGINAL CONTENT WITH CONTENT ACCESS CRITERIA
TRANSCODE CONTENT FOR MOBILE SUBSCRIBER DEVICE A
GENERATE/STORE CPK
PROTECT TRANSCODED CONTENT WITH CPK
GENERATE/STORE RIGHTS
GENERATE/STORE CONTENT ID OF TRANSCODED/PROTECTED CONTENT A
TRANSCODED/PROTECTED CONTENT A
CONTENT NOTIFICATION
CONTENT REQUEST
MOBILE SUBSCRIBER A
104
106
ORIGINAL CONTENT
CONTENT ID - ORIGINAL CONTENT
CONTENT ACCESS CRITERIA
CPK A
RIGHTS A
CONTENT ID – TRANSCODED /PROTECTED CONTENT A

Fig. 1C

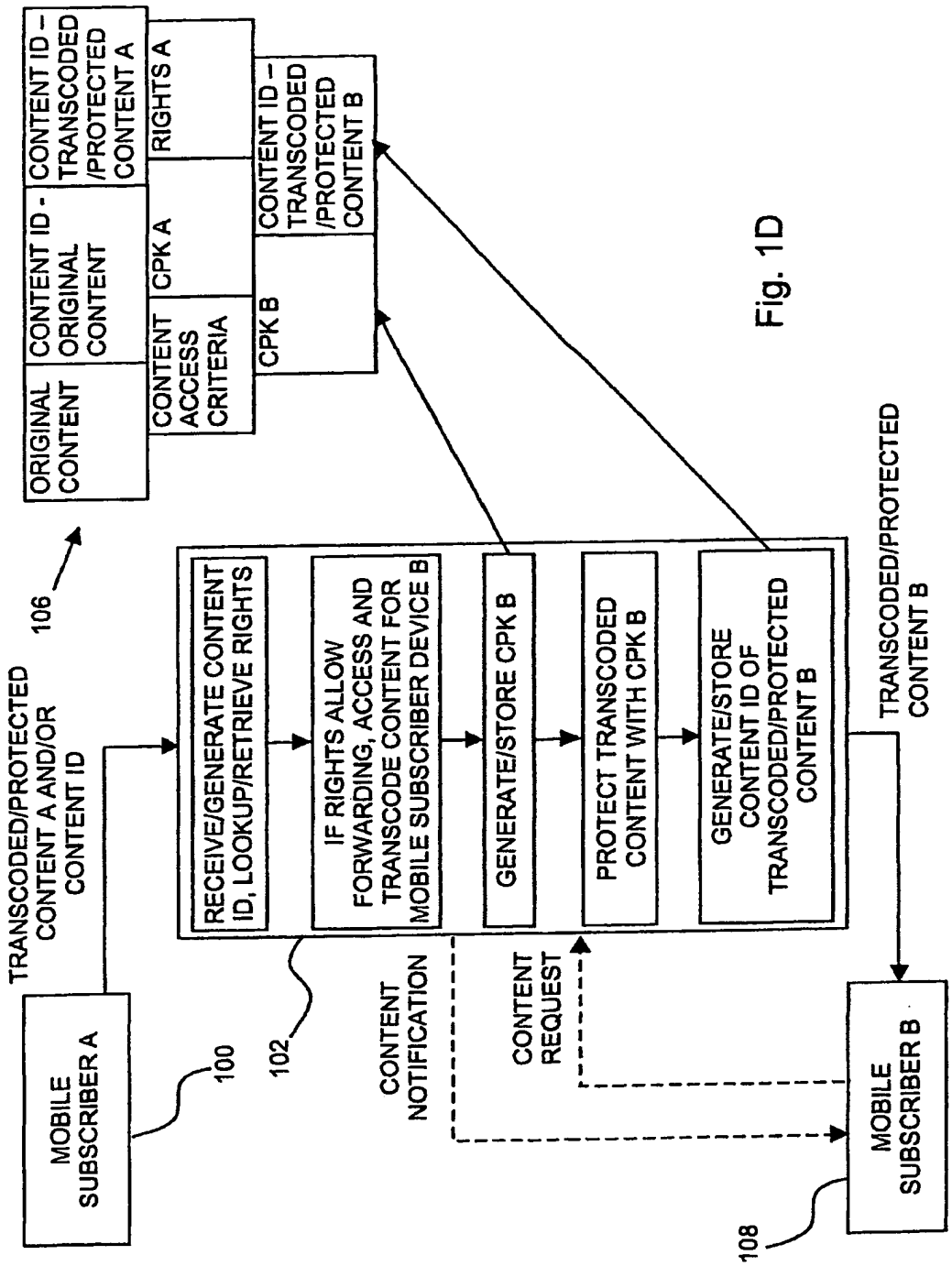

MOBILE SUBSCRIBER A
100
TRANSCODED/PROTECTED CONTENT A AND/OR CONTENT ID
102
RECEIVE/GENERATE CONTENT ID, LOOKUP/RETRIEVE RIGHTS
IF RIGHTS ALLOW FORWARDING, ACCESS AND TRANSCODE CONTENT FOR MOBILE SUBSCRIBER DEVICE B
GENERATE/STORE CPK B
PROTECT TRANSCODED CONTENT WITH CPK B
GENERATE/STORE CONTENT ID OF TRANSCODED/PROTECTED CONTENT B
TRANSCODED/PROTECTED CONTENT B
106
ORIGINAL CONTENT
CONTENT ID - ORIGINAL CONTENT
CONTENT ACCESS CRITERIA
CPK A
CPK B
RIGHTS A
CONTENT ID – TRANSCODED /PROTECTED CONTENT A
CONTENT ID – TRANSCODED /PROTECTED CONTENT B
CONTENT NOTIFICATION
CONTENT REQUEST
MOBILE SUBSCRIBER B
108

Fig. 1D

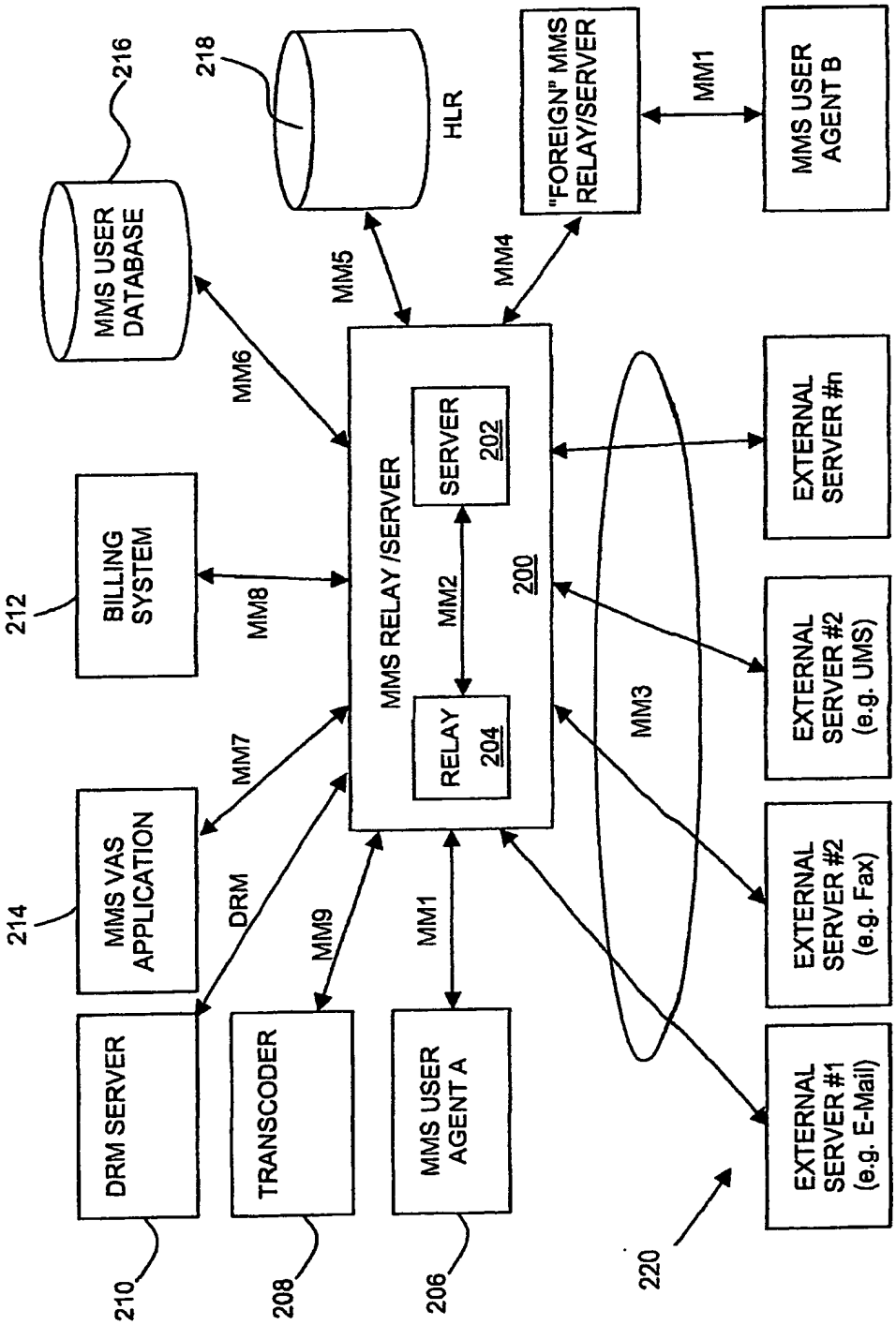

MMS USER DATABASE
216
HLR
218
"FOREIGN" MMS RELAY/SERVER
MM1
MMS USER AGENT B
MM6
MM5
MM4
MMS RELAY /SERVER
SERVER 202
200
RELAY 204
MM2
BILLING SYSTEM
212
MM8
EXTERNAL SERVER #n
MM7
MMS VAS APPLICATION
214
DRM
MM9
MM1
MM3
EXTERNAL SERVER #2 (e.g. UMS)
EXTERNAL SERVER #2 (e.g. Fax)
EXTERNAL SERVER #1 (e.g. E-Mail)
DRM SERVER
TRANSCODER
MMS USER AGENT A
210
208
206
220

Fig. 2

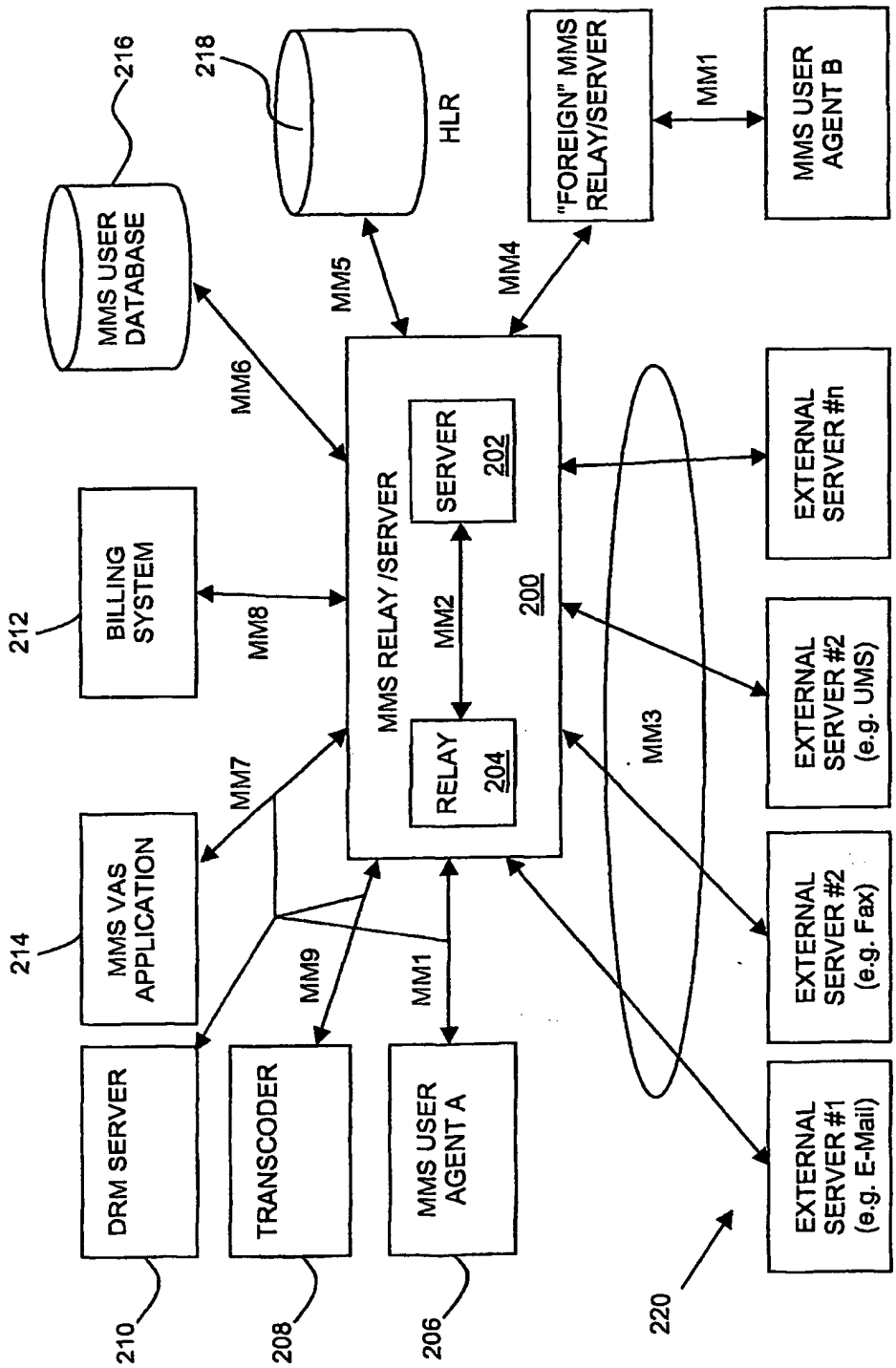

MMS USER DATABASE
216
HLR
218
"FOREIGN" MMS RELAY/SERVER
MM1
MMS USER AGENT B
MM6
MM5
MM4
MMS RELAY /SERVER
SERVER 202
200
MM2
RELAY 204
BILLING SYSTEM
212
MM8
EXTERNAL SERVER #n
MM7
MM3
EXTERNAL SERVER #2 (e.g. UMS)
MMS VAS APPLICATION
214
EXTERNAL SERVER #2 (e.g. Fax)
MM9
MM1
DRM SERVER
TRANSCODER
MMS USER AGENT A
EXTERNAL SERVER #1 (e.g. E-Mail)
210
208
206
220

Fig. 3

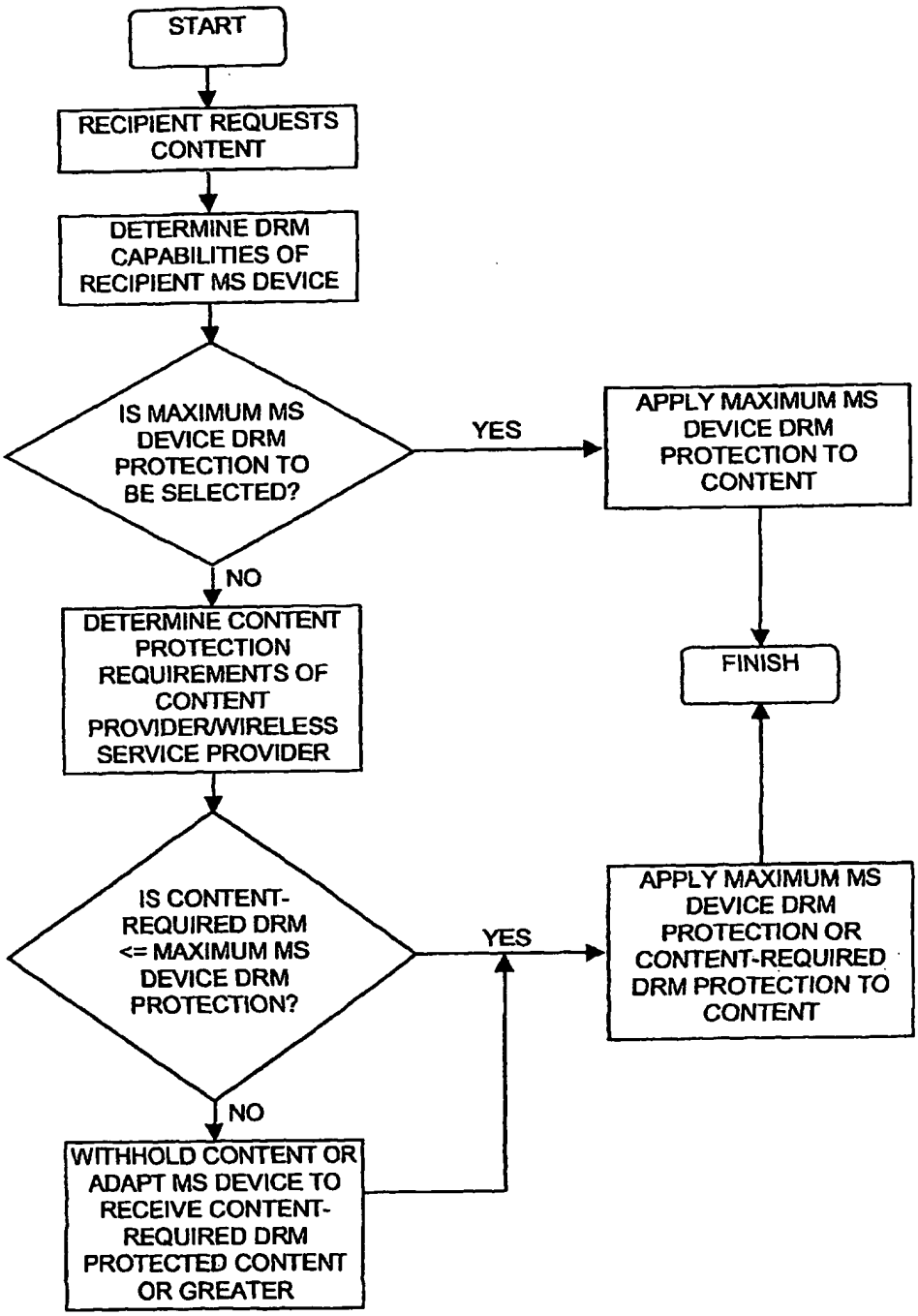

START
RECIPIENT REQUESTS CONTENT
DETERMINE DRM CAPABILITIES OF RECIPIENT MS DEVICE
IS MAXIMUM MS DEVICE DRM PROTECTION TO BE SELECTED?
YES
APPLY MAXIMUM MS DEVICE DRM PROTECTION TO CONTENT
NO
DETERMINE CONTENT PROTECTION REQUIREMENTS OF CONTENT PROVIDER/WIRELESS SERVICE PROVIDER
FINISH
IS CONTENT-REQUIRED DRM <= MAXIMUM MS DEVICE DRM PROTECTION?
YES
APPLY MAXIMUM MS DEVICE DRM PROTECTION OR CONTENT-REQUIRED DRM PROTECTION TO CONTENT
NO
WITHHOLD CONTENT OR ADAPT MS DEVICE TO RECEIVE CONTENT-REQUIRED DRM PROTECTED CONTENT OR GREATER

Fig. 4

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/589,417	11/07/2006	David Mail	7251/94662	8225

24628 7590 05/20/2010

Husch Blackwell Sanders, LLP
Husch Blackwell Sanders LLP Welsh & Katz
120 S RIVERSIDE PLAZA
22ND FLOOR
CHICAGO, IL 60606

EXAMINER	
CHAO, MICHAEL W	

ART UNIT	PAPER NUMBER
2442	

MAIL DATE	DELIVERY MODE
05/20/2010	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/589,417	MAIL ET AL.	
	Examiner	Art Unit	
	Michael Chao	2442	

– The MAILING DATE of this communication appears on the cover sheet with the correspondence address –

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *20 April 2010*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,3-14,17-21,26-29,31-42,45-49 and 58-60* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,3-14,17-21,26-29,31-42,45-49 and 58-60* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

This action is in response to applicant's arguments filed 5/06/2010, which was in response to USPTO Office Action mailed 1/06/2010.

Claims 1, 3-14, 17-21, 26-29, 31-42, 45-49 and 58-60 are pending.

Response to Arguments

Applicant's arguments filed 4/20/2010 have been fully considered but they are not persuasive.

Applicant's argument (page 12) that Warsta in view of Malik does not teach "storing said content ID of said firstly transcoded version of multimedia content, as a stored first content ID, in association with said stored multimedia content", stated another way, storing the content ID of a transcoded version of a media in association with the untranscoded media, is not persuasive. Warsta explicitly recites that versions of content are indexed by content ID and terminal type (Warsta paragraph [0058]). Since the content ID identifies both the transcoded content and the original content, the content ID of the transcoded content (content ID and terminal type) is 'in association' with the untranscoded media. This is because the content ID may be used to identify the untranscoded content.

Applicant further argues (paragraph 2 page 13) that the cited paragraph of Warsta (pargraph [58]) does not show the content ID of the transcoded version in association with the stored multimedia content (untranscoded content). However,

contrary to Applicants assertion (last line of page 12) that association means stored with, association merely requires that there be some relation between the two. As seen above, the content ID indicates the untranscoded version; thus the adapted contents (content ID and terminal type) tuple is associated with the untranscoded content.

Applicant's argument (paragraph 3 page 13) that claim 1 does *not* recite elements of Warsta, is irrelevant because the transitional phrase 'comprising' is open ended. 'Comprising' does not limit the claim to recited elements; therefore, it may be mapped to prior art which contains further elements or steps than those recited by the claim. (See MPEP 2111.03)

Applicant's argument (page 13) that Warsta in view of Malik does not teach "using said stored first content ID of said firstly transcoded version of said multimedia content" and "comparing said received content ID with said stored first content ID", is not persuasive.

Applicant further argues that Malik's attachment cache is only capable of finding an attachment which is identical to an attachment in a received e-mail message, and is thus incapable of generating the received content ID and comparing it to the stored content ID.

To review, Warsta discloses a multi-version content cache. Malik discloses caching attachments and comparing received attachment to stored attachments by checksum determination or comparing header information. Therefore the combination of Warsta in view of Malik yields a multi-version content cache that can compare incoming attachments to stored attachments. Warsta recites a method of determining whether

content is stored in the cache (Figure 7 and also paragraph [0061]+) where the content is compared using content ID and terminal type (Figure 6) to determine if a version is cached. Malik's comparison is shown in column 5 line 35. The combination of Warsta in view of Malik would then check for attachments using content ID and terminal type, and when no attachment is found, a new content adaptation is performed (Warsta paragraph [0062]). Therefore, the combination of Warsta in view of Malik teaches the argued lacking elements, in that if it determines the cache does not have a required version of a media, it creates said version for the second media device (the forwarded to device, Malik column 2 line 15)

Applicant's argument (page 14-15) that Malik teaches away from the recited: "receiving . . . an instruction to forward said item of multimedia content to a second multimedia device, said instruction comprising a copy of said firstly transcoded version of said multimedia content . . ." because Malik discloses replacing large attachments with pointers, is not persuasive. Applicant's argued portion of Malik (column 3 lines 50-60) recites "when the e-mail server receives an e-mail attachment file that is larger than a threshold size, the server performs a database search for another copy of the attachment file in the mail store. If another copy is located, the system creates a pointer in the mail store". Stated another way, when the mail server of Malik receives an email with an attachment, it prevents duplicates by creating a pointer to a prior stored attachment (see also column 6). This process appears unrelated to applicants argued "instruction to forward said item of multimedia content . . . comprising a copy of said firstly transcoded version" since the pointer is generated at the mail server, and does

not appear to change the operation of the client system. Moreover, the recitation that "when the e-mail server receives an e-mail attachment . . . performs a database search" explicitly states that the server expects the copy of said multimedia content. Applicant's argument is not persuasive.

Applicant's further arguments depend on those addressed and are not persuasive for the reasons stated.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1, 3-14, 29, 31-42, are rejected under 35 U.S.C. 103(a) as being unpatentable over Warsta et al. (US 2004/0181550, cited in OA dated 7/06/2009), in view of Malik (US 7,003,551, cited in OA dated 7/06/2009).

With respect to claims 1, 29 Warsta teaches: A method for distributing multimedia content, the method comprising:

Storing an item of multimedia content as stored multimedia content at a multimedia message center (MMSC); ("MMSC is responsible for storing incoming and outgoing MMS messages, as well as the transfer of messages between different messaging systems" Warsta paragraph [0044])

Firstly transcoding ("the adaptation of content is performed in accordance with the received capabilities" Warsta paragraph [0010]) said multimedia content for playback on a first multimedia device, thereby producing a firstly transcoded version of said multimedia content; ("The requesting network device capabilities are compared to previous requesting network device capabilities, such that if a capability match is found, previously adapted content may be transmitted to the requesting network device" And generally Warsta paragraph [0024])

Generating a content ID of said firstly transcoded version of said multimedia content; ("the adapted content is cached within database 616 and indexed according to content ID and terminal type" Warsta paragraph [0058])

Storing said content ID of said firstly transcoded version of said multimedia content, as a stored first content ID, in association with said stored multimedia content; ("the adapted content is cached within database 616 and indexed according to content ID and terminal type" Warsta paragraph [0058])

Transcoding said stored multimedia content for playback on said second multimedia device ("The requesting network device capabilities are compared to previous requesting network device capabilities, such that if a capability match is found, previously adapted content may be transmitted to the requesting network device, obviating the need for an additional adaptation." And generally Warsta paragraph [0024]; Also, "Not only are network elements 108 and 110 capable of caching or otherwise storing content 104, but they are also able to cache/store

(hereinafter "cache") the various adaptations of content 104" Warsta paragraph [0029])

Warsta does not explicitly recite:

Receiving, at said MMSC an instruction to forward said item of multimedia content to a second multimedia device, said instruction comprising a copy of said firstly transcoded version of said multimedia content; and

Performing the following in response to said instruction:

Accessing said stored content using said stored first content ID of said firstly transcoded version of said multimedia content, said accessing comprising:

Generating a received content ID of said copy of said firstly transcoded version of said multimedia content; and

Looking up said stored multimedia content by comparing said received content ID with said stored first content ID; and

Malik teaches such lacking elements:

Receiving, at said MMSC an instruction to forward said item of multimedia content to a second multimedia device, said instruction comprising a copy of said firstly transcoded version of said multimedia content; and ("Some of the recipients may in turn forward this e-mail communication to other groups of recipients." Malik column 2 line 15)

Performing the following in response to said instruction:

Accessing said stored content using said stored first content ID of said firstly transcoded version of said multimedia content, said accessing comprising:

Generating a received content ID of said copy of said firstly transcoded version of said multimedia content; and ("The duplication checker next identifies the properties associated with the attachment file in the file header" Malik column 6 line 35)

Looking up said stored multimedia content by comparing said received content ID with said stored first content ID; and ("processing step generates information by which the attachment file comparison section 26 of the duplication checker 24 can search the attachment file storage database 28 for identical attachment files" Malik column 5 line 35)

A person of ordinary skill in the art at the time of invention would have combined Warsta with Malik by including the mail store (item 23 figure 2 of Malik) with the MMSC (item 320 of figure 3 of Warsta) to store attachments (item 29a figure 2 of Malik) and content (Figure 5 of Warsta), thereby allowing forwarding and content ID lookups of Malik by including a message table with forwarding functionality as described in Malik in the invention of Warsta. It would have been obvious at the time the invention was made to a person of ordinary skill in the art to include a 'mail store' in Warsta in order to consolidate the storage for forwarded communications (Malik column 2 line 40).

With respect to claims 3, 31 Warsta teaches: wherein said storing an item of multimedia content comprises storing said item of multimedia content together with an original content identifier (ID) identifying said content. ("the adapted content is cached

within database 616 and indexed according to content ID and terminal type" Warsta paragraph [0058])

With respect to claims 4, 32 Warsta in view of Malik teaches: wherein said storing an item of multimedia content comprises storing said item of multimedia content together with an original content identifier (ID) that uniquely identifies said content. ("the adapted content is cached within database 616 and indexed according to content ID and terminal type" Warsta paragraph [0058]; Also "such as checksum determination" Malik column 5 line 30)

With respect to claims 5, 33 Warsta in view of Malik teaches: storing said item of multimedia content in its original form. ("Not only are network elements 108 and 110 capable of caching or otherwise storing content 104, but they are also able to cache/store (hereinafter "cache") the various adaptations of content 104" Warsta paragraph [0029]; Also "stores the attachment file" Malik column 5 line 40)

With respect to claims 6, 34 Warsta in view of Malik teaches: storing said item of multimedia content such that said content may be partly or wholly reconstituted. ("Not only are network elements 108 and 110 capable of caching or otherwise storing content 104, but they are also able to cache/store (hereinafter "cache") the various adaptations of content 104" Warsta paragraph [0029]; Also "The mail store then creates a link in the record of the header database to the attachment in the cache portion" Malik column 5 line 61)

With respect to claims 7, 35 Warsta in view of Malik teaches: receiving said original content ID from a provider of said content. (See Warsta Figure 5 content IDs as

filenames; also "The duplication checker next identifies the properties associated with the attachment file in the file header, which may include any of: title/name . . ." Malik column 6 line 35)

With respect to claims 8, 36 Warsta in view of Malik teaches: further comprising generating said original content ID by applying either of a predefined hashing method and a predefined fingerprinting method to said content and using either of the resulting hash and fingerprint as said original content ID. ("the adapted content is cached within database 616 and indexed according to content ID and terminal type" Warsta paragraph [0058]; also "such as checksum determination" Malik column 5 line 30)

Regarding claims 9, 37, Warsta teaches: associating said original content ID with different transcoded versions of said content. ("the adapted content is cached within database 616 and indexed according to content ID and terminal type" Warsta paragraph [0058])

Regarding claims 10, 38, Warsta teaches: sending a notification to said first multimedia device indicating that said content is available for download to said multimedia device. ("The M-Notification.ind inform mobile terminal 316 about the contents of received message 326 and its purpose is to allow mobile terminal 316 to fetch multimedia message 326 from MMSC 320" Warsta paragraph [0050])

Regarding claims 11, 39, Warsta teaches: delivering said firstly transcoded content to said first multimedia device in an MMS message. ("The messaging capabilities include mobile originated messages sent to other mobile terminals or

applications and application originated messages sent to mobile terminals or other applications" Warsta paragraph [0044]; See also Warsta paragraph [0033])

Regarding claims 12, 40, Warsta in view of Malik teaches: delivering said firstly transcoded content to said first multimedia device, in an mms message, together with any of said content IDs. ("extraction of certain attachment file header information." Malik column 5 line 30)

Regarding claims 13, 41, Warsta in view of Malik teaches: receiving said firstly transcoded content from said multimedia device in an MMS message; and ("Some of the recipients may in turn forward this e-mail communication to other groups of recipients." Malik column 2 line 15)

Regenerating said content ID of said firstly transcoded content. ("generate file identification information. . . . such as checksum determination, or extraction of certain attachment file header information." Malik column 5 line 30; Also "The duplication checker next identifies the properties associated with the attachment file in the file header" Malik column 6 line 35)

Regarding claims 14, 42, Warsta in view of Malik teaches: wherein said regenerating step comprises regenerating said content ID of said firstly transcoded content using the same method used to generate said content ID of said firstly transcoded content. ("generate file identification information. . . . such as checksum determination, or extraction of certain attachment file header information." Malik column 5 line 30)

Claims 17-21, 26-28, 45-49, are rejected under 35 U.S.C. 103(a) as being unpatentable over Warsta et al. (US 2004/0181550), in view of Malik (U.S. 7,003,551), in view of Kobata (US 2002/0077986).

With respect to claims 17, 45, Warsta in view of Malik does not teach protecting transcoded content with a content protection key (CPK). Kobata teaches said limitation, "the digital asset may be stored in an encrypted format. . . decrypting the digital asset may include retrieving a key from the intermediate server" (Kobata paragraph [0035]). A person of ordinary skill in the art would have modified Warsta in view of Malik with Kobata by including in the message table a digital rights manager of the form described in Kobata. It would have been obvious at the time the invention was made to a person of ordinary skill in the art to modify the combination to provide "secure [] communication and control of digital assets" (Kobata Abstract)

With respect to claims 18, 46, Warsta in view of Malik does not teach identifying any rights associated with providing said content to any of said multimedia devices;

Generating at least one entitlement as a function of said rights; and

Providing said content to any of said multimedia devices in accordance with said entitlement. ("Furthermore depending on the digital rights defined for a particular copy or form of digital content 320, the end-user may be able to forward the digital content" Kobata paragraph [0124]). A person of ordinary skill in the art would have modified Warsta in view of Malik with Kobata by including in the message table a digital rights manager of the form described in Kobata. It would have been obvious at the time the

invention was made to a person of ordinary skill in the art to modify the combination to provide "secure [] communication and control of digital assets" (Kobata Abstract)

With respect to claims 19, 47, Warsta in view of Malik does not teach determining if said copy of said firstly transcoded content is protected;

If said copy is protected, determining if said content may be forwarded to said second multimedia device as indicated by any rights associated with either rof said content and the recipient of said firstly transcoded content; and

If said content may be forwarded, protecting and forwarding said secondly transcoded content to said second multimedia device. ("Furthermore depending on the digital rights defined for a particular copy or form of digital content 320, the end-user may be able to forward the digital content" Kobata paragraph [0124]). A person of ordinary skill in the art would have modified Warsta in view of Malik with Kobata by including in the message table a digital rights manager of the form described in Kobata. It would have been obvious at the time the invention was made to a person of ordinary skill in the art to modify the combination to provide "secure [] communication and control of digital assets" (Kobata Abstract)

With respect to claims 20, 48, Warsta in view of Malik in view of Kobata teaches: protecting said secondly transcoded content with a content protection key (CPK) associated with said secondly transcoded content. ("The tracking techniques may be employed to implement "super-distributions" in which users to which a digital asset is distributed are authorized to redistribute the digital asset to other users (though perhaps with more limited rights)." Kobata paragraph [0021])

With respect to claims 21, 49, Warsta in view of Malik in view of Kobata teaches: wherein said fist determining step comprises determining that said copy of said firstly transcoded content is protected by identifying a CPK stored in association with the content ID. ("As an alternative, rights may be stored locally but separately from the digital asset with a link to the digital asset" Kobata paragraph [0023])

With respect to claim 26, Warsta teaches: A multimedia content distribution system comprising:

An MMS server;

An MMS relay; ("MMSC" Warsta paragraph [0044]. MMSC as defined by the applicant includes an MMS server which controls storage (Warsta paragraph [0044]) and an MMS relay which controls transcoding (Warsta paragraph [0052]) and delivery (Warsta paragraph [0044]))

A transcoder; and ("For each distinct mobile terminal capability type, a content adaptation is prepared for each mobile terminal capability type" And generally Warsta paragraph [0061])

Wherein said MMS server, MMS relay, transcoder are individually or cooperatively operative to:

Store an item of multimedia content as stored multimedia content; ("MMSC is responsible for storing incoming and outgoing MMS messages, as well as the transfer of messages between different messaging systems" Warsta paragraph [0044])

Firstly transcode said multimedia content for playback on a first multimedia device, thereby producing a firstly transcoded version of said multimedia content; ("The requesting network device capabilities are compared to previous requesting network device capabilities, such that if a capability match is found, previously adapted content may be transmitted to the requesting network device" And generally Warsta paragraph [0024])

Generate a content ID of said firstly transcoded version of said multimedia content;

Store said content ID of said firstly transcoded version of said multimedia content, as stored first content ID, in association with said stored multimedia content; ("the adapted content is cached within database 616 and indexed according to content ID and terminal type" Warsta paragraph [0058])

transcode said stored multimedia content for playback on said second multimedia device content for playback on said second multimedia device. ("The requesting network device capabilities are compared to previous requesting network device capabilities, such that if a capability match is found, previously adapted content may be transmitted to the requesting network device, obviating the need for an additional adaptation." And generally Warsta paragraph [0024]; Also, "Not only are network elements 108 and 110 capable of caching or otherwise storing content 104, but they are also able to cache/store (hereinafter "cache") the various adaptations of content 104" Warsta paragraph [0029])

Warsta does not explicitly recite:

A DRM server,

Receive an instruction, via a multimedia message service (MMS) message, to forward said item of multimedia content to a second multimedia device, said instruction comprising a copy of said firstly transcoded version of said multimedia content; and

perform the following in response to said instruction:

access said stored content using said stored first content ID of said firstly transcoded version of said multimedia content, comprising:

generating a received content ID of said stored copy of said firstly transcoded version of said multimedia content; and

looking up said stored multimedia by comparing said received content ID with said stored first content ID; and

Malik teaches:

Receive an instruction, via a multimedia message service (MMS) message, to forward said item of multimedia content to a second multimedia device, said instruction comprising a copy of said firstly transcoded version of said multimedia content; and ("Some of the recipients may in turn forward this e-mail communication to other groups of recipients." Malik column 2 line 15)

perform the following in response to said instruction:

access said stored content using said stored first content ID of said firstly transcoded version of said multimedia content, comprising:

generating a received content ID of said stored copy of said firstly transcoded version of said multimedia content; and ("The duplication checker next

identifies the properties associated with the attachment file in the file header" Malik column 6 line 35)

looking up said stored multimedia by comparing said received content ID with said stored first content ID; and ("processing step generates information by which the attachment file comparison section 26 of the duplication checker 24 can search the attachment file storage database 28 for identical attachment files" Malik column 5 line 35)

A person of ordinary skill in the art at the time of invention would have combined Warsta with Malik by including the mail store (item 23 figure 2 of Malik) with the MMSC (item 320 of figure 3 of Warsta) to store attachments (item 29a figure 2 of Malik) and content (Figure 5 of Warsta), thereby allowing forwarding and content ID lookups of Malik by including a message table with forwarding functionality as described in Malik in the invention of Warsta. It would have been obvious at the time the invention was made to a person of ordinary skill in the art to include a 'mail store' in Warsta in order to consolidate the storage for forwarded communications (Malik column 2 line 40).

Furthermore, Warsta in view of Malik does not disclose A DRM server.

Kobata teaches a DRM server: "Fig. 3 shows a computer device 310 in communication with a server-based global rights manager unit" (Kobata paragraph [0116]). A person of ordinary skill in the art would have modified Warsta in view of Malik with Kobata by including in the message table a digital rights manager of the form described in Kobata. It would have been obvious at the time the invention was made to

a person of ordinary skill in the art to modify the combination to provide "secure [] communication and control of digital assets" (Kobata Abstract)

With respect to claim 27, Warsta in view of Malik in view of Kobata teaches: wherein any of said MMS server, MMS relay, transcoder, and DRM server are individually or cooperatively operative to track whom said content is sent and with what rights. ("The server may maintain a virtual database of digital assets and may use the database in implementing functions such as data mining, tracking, and monitoring of rights consumption" Kobata paragraph [0018])

With respect to claim 28, Warsta in view of Malik in view of Kobata teaches: wherein said DRM server acts as either of a probe and a proxy between any of said MMS server, said MMS relay, and said transcoder. ("The server-based approach to communicating digital assets provides a number of other advantages. . . . it may be used to control digital asset delivery. . ." Kobata paragraph [0024])

Claims 58-60 are rejected under 35 U.S.C. 103(a) as being unpatentable over Warsta et al. (US 2004/0181550), in view of Malik (US 7,003,551), in view of Mattis et al. (US 6,128,623, cited in OA dated 7/06/2009)

With respect to claim 58-60, Warsta in view of Malik teaches: wherein said generating a content ID of said firstly transcoded version of said multimedia content comprises:

Applying either of the following to said firstly transcoded version of said multimedia content, and producing a result:

A predefined hashing method; and

A predefined fingerprinting method; and ("generate file identification information. . . . such as checksum determination, or extraction of certain attachment file header information." Malik column 5 line 30)

Using said result as said [received] content ID.

Warsta in view of Malik does not teach that the content ID and the received content ID are fingerprinted/hashed, while "looking up said stored multimedia content by comparing said received content ID with said stored first content ID" as recited in claim 1. Mattis teaches such an element. "this two-level indexing structure facilitates the ability to associate multiple alternate objects with a single name" (Mattis column 8 line 23). "Unlike other cache systems that use the name or URL of an object as the key by which the object is referenced, embodiments of the invention use a "fingerprint" of the content that makes up the object itself, to locate the object." (Mattis column 8 line 28). "each name key in the directory table 110 maps to one of the vectors of alternates 122a-n, which enable the cache to select one version of an object from among a plurality of related versions. For example, the object 52 may be a Web page ad server 40 can store versions of the object in the English, French, and Japanese languages." (Mattis column 14 line 33). A person of ordinary skill in the art would have modified Warsta in view of Malik by using duplicate detection according to the 'fingerprint' method of Mattis, and further included the two-level indexing of Mattis by incorporating the relevant data structures into the cache of Warsta in view of Malik. It would have been obvious at the

time the invention was made to a person of ordinary skill in the art to modify Warsta in view of Malik with Mattis in order to have an efficient web proxy.

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael Chao whose telephone number is (571)270-5657. The examiner can normally be reached on 8-4 Monday through Thursday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Philip Lee can be reached on (571)272-3967. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/M. C./
Examiner, Art Unit 2442

/Philip C Lee/
Acting Supervisory Patent Examiner, Art Unit 2442

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/589,417	11/07/2006	David Mail	7251/94662	8225

24628 7590 07/29/2010

Husch Blackwell Sanders, LLP
Husch Blackwell Sanders LLP Welsh & Katz
120 S RIVERSIDE PLAZA
22ND FLOOR
CHICAGO, IL 60606

EXAMINER	
CHAO, MICHAEL W	

ART UNIT	PAPER NUMBER
2442	

MAIL DATE	DELIVERY MODE
07/29/2010	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Advisory Action Before the Filing of an Appeal Brief	**Application No.** 10/589,417	**Applicant(s)** MAIL ET AL.	
	Examiner Michael Chao	**Art Unit** 2442	

--The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

THE REPLY FILED 20 July 2010 FAILS TO PLACE THIS APPLICATION IN CONDITION FOR ALLOWANCE.

1. ☒ The reply was filed after a final rejection, but prior to or on the same day as filing a Notice of Appeal. To avoid abandonment of this application, applicant must timely file one of the following replies: (1) an amendment, affidavit, or other evidence, which places the application in condition for allowance; (2) a Notice of Appeal (with appeal fee) in compliance with 37 CFR 41.31; or (3) a Request for Continued Examination (RCE) in compliance with 37 CFR 1.114. The reply must be filed within one of the following time periods:
   a) ☐ The period for reply expires _____months from the mailing date of the final rejection.
   b) ☒ The period for reply expires on: (1) the mailing date of this Advisory Action, or (2) the date set forth in the final rejection, whichever is later. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of the final rejection.

   Examiner Note: If box 1 is checked, check either box (a) or (b). ONLY CHECK BOX (b) WHEN THE FIRST REPLY WAS FILED WITHIN TWO MONTHS OF THE FINAL REJECTION. See MPEP 706.07(f).

Extensions of time may be obtained under 37 CFR 1.136(a). The date on which the petition under 37 CFR 1.136(a) and the appropriate extension fee have been filed is the date for purposes of determining the period of extension and the corresponding amount of the fee. The appropriate extension fee under 37 CFR 1.17(a) is calculated from: (1) the expiration date of the shortened statutory period for reply originally set in the final Office action; or (2) as set forth in (b) above, if checked. Any reply received by the Office later than three months after the mailing date of the final rejection, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

NOTICE OF APPEAL

2. ☐ The Notice of Appeal was filed on _____. A brief in compliance with 37 CFR 41.37 must be filed within two months of the date of filing the Notice of Appeal (37 CFR 41.37(a)), or any extension thereof (37 CFR 41.37(e)), to avoid dismissal of the appeal. Since a Notice of Appeal has been filed, any reply must be filed within the time period set forth in 37 CFR 41.37(a).

AMENDMENTS

3. ☐ The proposed amendment(s) filed after a final rejection, but prior to the date of filing a brief, will not be entered because
   (a) ☐ They raise new issues that would require further consideration and/or search (see NOTE below);
   (b) ☐ They raise the issue of new matter (see NOTE below);
   (c) ☐ They are not deemed to place the application in better form for appeal by materially reducing or simplifying the issues for appeal; and/or
   (d) ☐ They present additional claims without canceling a corresponding number of finally rejected claims.

   NOTE: _____. (See 37 CFR 1.116 and 41.33(a)).
4. ☐ The amendments are not in compliance with 37 CFR 1.121. See attached Notice of Non-Compliant Amendment (PTOL-324).
5. ☐ Applicant's reply has overcome the following rejection(s): _____.
6. ☐ Newly proposed or amended claim(s) _____ would be allowable if submitted in a separate, timely filed amendment canceling the non-allowable claim(s).
7. ☒ For purposes of appeal, the proposed amendment(s): a) ☐ will not be entered, or b) ☒ will be entered and an explanation of how the new or amended claims would be rejected is provided below or appended.
   The status of the claim(s) is (or will be) as follows:
   Claim(s) allowed: _____.
   Claim(s) objected to: _____.
   Claim(s) rejected: *1,3-14,17-21,26-29,31-42,45-49 and 58-60*.
   Claim(s) withdrawn from consideration: _____.

AFFIDAVIT OR OTHER EVIDENCE

8. ☐ The affidavit or other evidence filed after a final action, but before or on the date of filing a Notice of Appeal will not be entered because applicant failed to provide a showing of good and sufficient reasons why the affidavit or other evidence is necessary and was not earlier presented. See 37 CFR 1.116(e).
9. ☐ The affidavit or other evidence filed after the date of filing a Notice of Appeal, but prior to the date of filing a brief, will not be entered because the affidavit or other evidence failed to overcome all rejections under appeal and/or appellant fails to provide a showing a good and sufficient reasons why it is necessary and was not earlier presented. See 37 CFR 41.33(d)(1).
10. ☐ The affidavit or other evidence is entered. An explanation of the status of the claims after entry is below or attached.

REQUEST FOR RECONSIDERATION/OTHER

11. ☒ The request for reconsideration has been considered but does NOT place the application in condition for allowance because: See Continuation Sheet.
12. ☒ Note the attached Information *Disclosure Statement*(s). (PTO/SB/08) Paper No(s). _____
13. ☒ Other: See Continuation Sheet.

/Asad M Nawaz/
Supervisory Patent Examiner, Art Unit 2442

Continuation of 11. does NOT place the application in condition for allowance because: Applicant's request for reconsideration is not persuasive and sufficiently addressed in Final Office Action dated 5/20/2010. Further, the argument that Warsta in view of Malik does not teach storing the original version of the content is not persuasive. Briefly, Warsta teaches a multi-version media cache and Malik teaches storing received attachments and comparing them to prior stored attachments. Warsta contemplates looking up content using an ID and a terminal type [paragraph 58] and Malik, as cited in the Final Office Action, teaches storing the 'original' version of the messages and looking them up (Malik column 6 line 35 and column 5 line 35). Thus the combination of Warsta in view of Malik teaches a multi version media cache that uses content ID and terminal type to look up content and stores the original version.

Continuation of 13. Other: The IDS filed 5/27/2010 accompanied by both fee and statement as required by § 1.97 (d) has been considered.

US 20040181550A1

(19) **United States**

(12) **Patent Application Publication** (10) **Pub. No.: US 2004/0181550 A1**

Warsta et al. (43) **Pub. Date: Sep. 16, 2004**

(54) **SYSTEM AND METHOD FOR EFFICIENT ADAPTATION OF MULTIMEDIA MESSAGE CONTENT**

(76) Inventors: **Ville Warsta**, Helsinki (FI); **Teppo Savinen**, Vihti (FI); **Petri Timonen**, Espoo (FI)

Correspondence Address:
Crawford Maunu PLLC
1270 Northland Drive, Suite 390
St. Paul, MN 55120 (US)

(21) Appl. No.: **10/388,209**

(22) Filed: **Mar. 13, 2003**

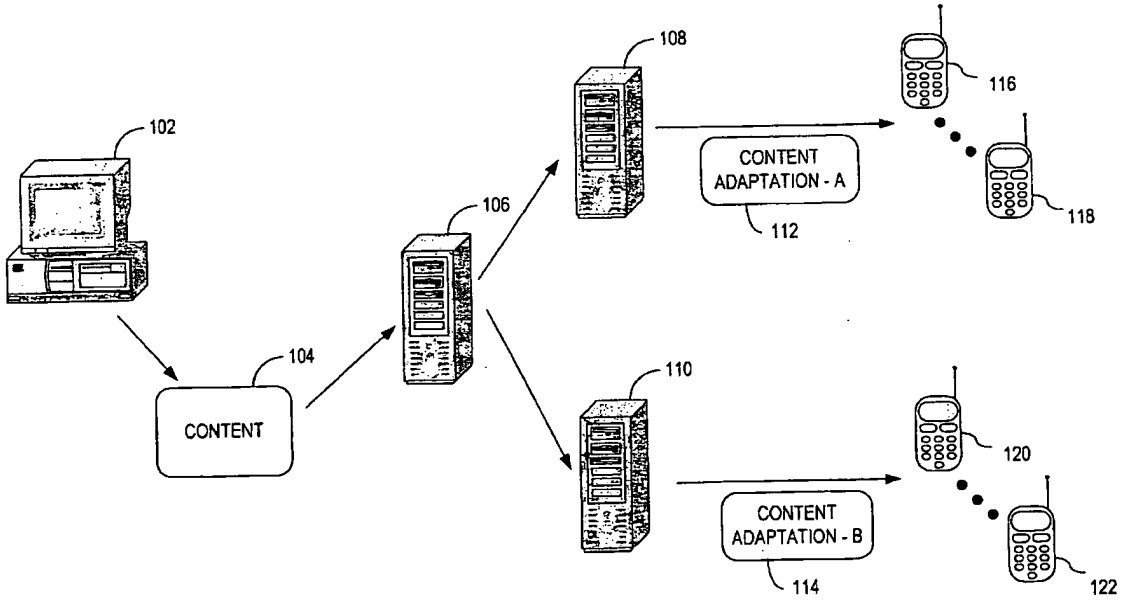
Publication Classification

(51) **Int. Cl.**[7] **G06F 17/00**

(52) **U.S. Cl.** **707/104.1**

(57) **ABSTRACT**

A system and method for providing previously adapted content to requesting network devices. The requesting network device capabilities are compared to the previous requesting network device capabilities, such that if a capability match is found, previously adapted content may be transmitted to the requesting network device, obviating the need for an additional adaptation. In another embodiment, a pre-adaptation method is employed, whereby content adaptations for all known network device capabilities are cached for future use.



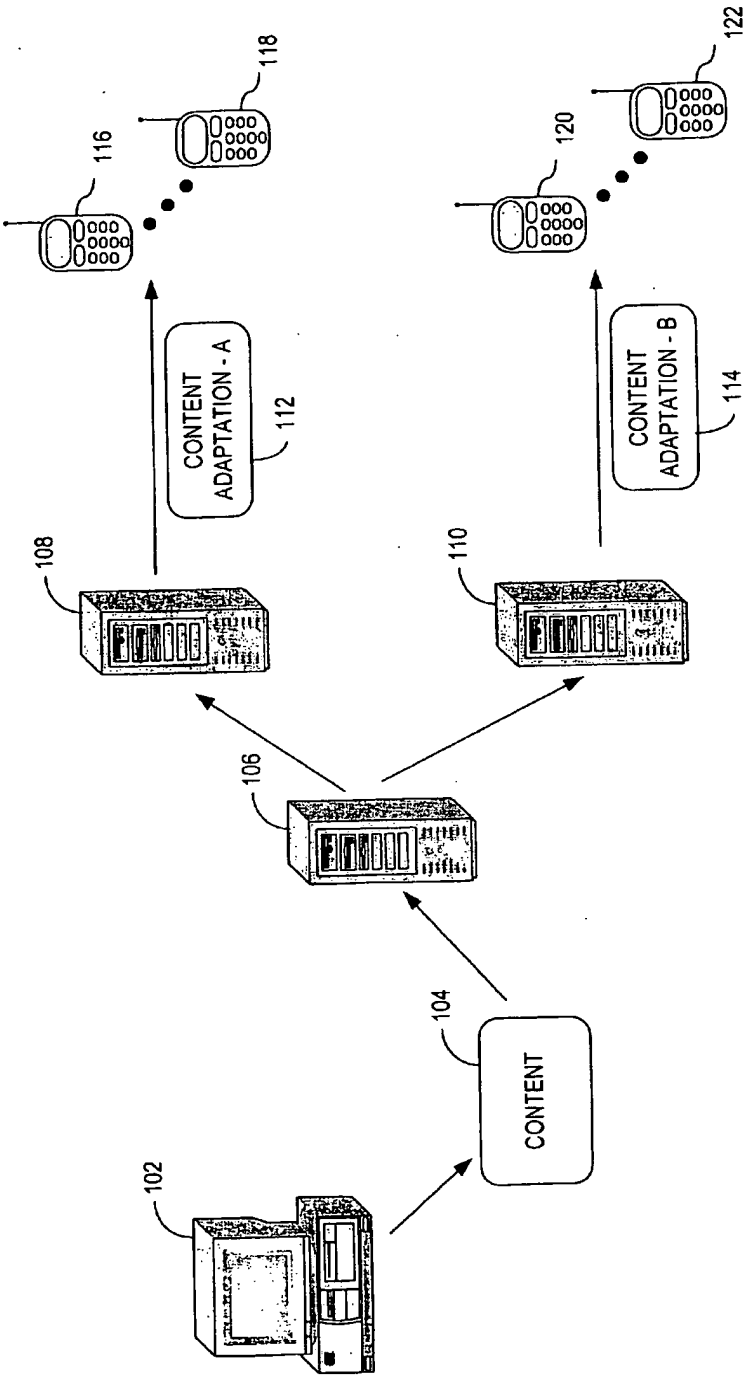

102
104
CONTENT
106
108
110
112
CONTENT ADAPTATION - A
114
CONTENT ADAPTATION - B
116
118
120
122

FIG. 1

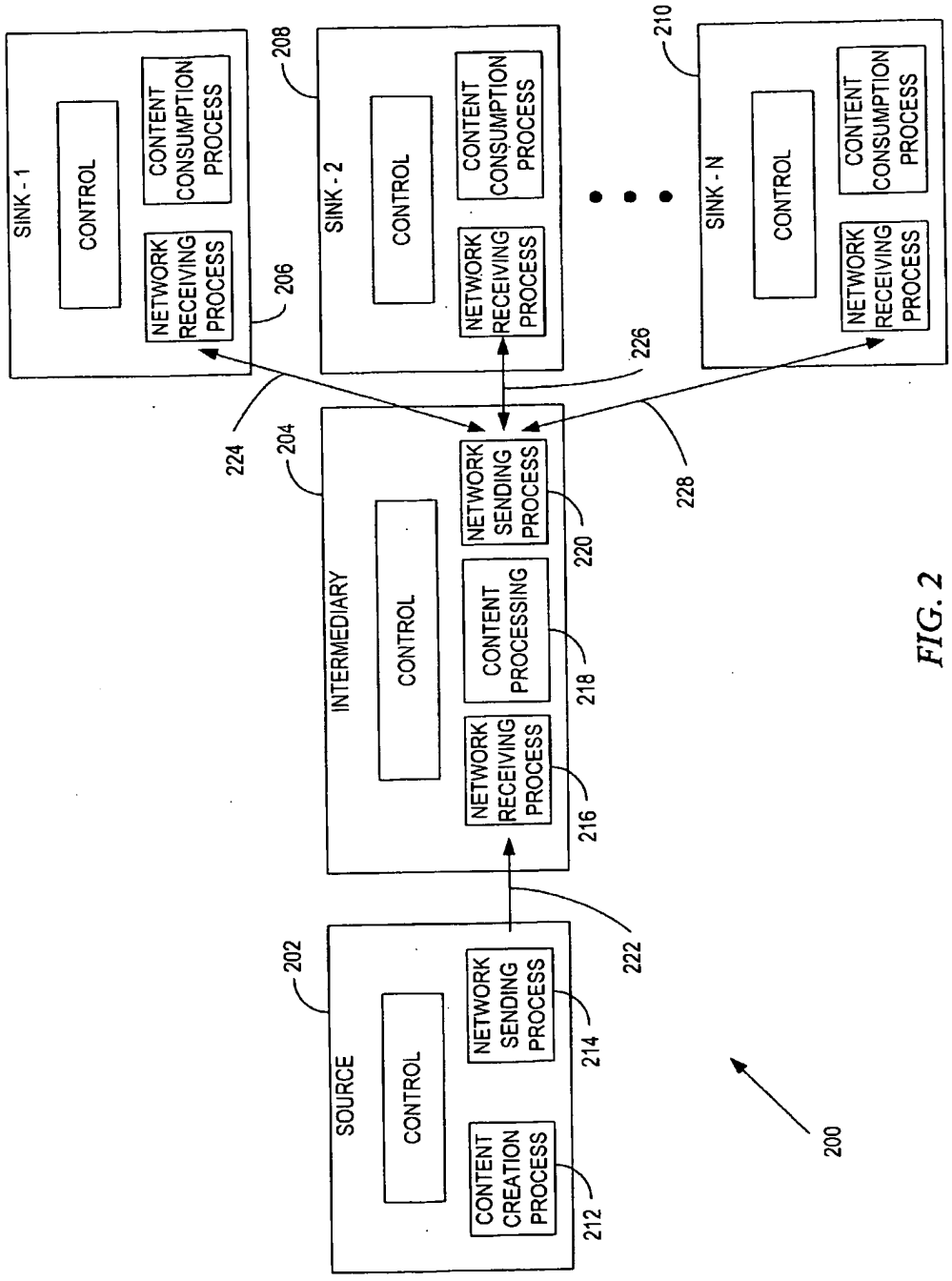

SINK - 1
CONTROL
CONTENT CONSUMPTION PROCESS
NETWORK RECEIVING PROCESS
206
208
SINK - 2
CONTROL
CONTENT CONSUMPTION PROCESS
NETWORK RECEIVING PROCESS
210
SINK - N
CONTROL
CONTENT CONSUMPTION PROCESS
NETWORK RECEIVING PROCESS
224
226
228
204
INTERMEDIARY
CONTROL
NETWORK SENDING PROCESS
220
CONTENT PROCESSING
218
NETWORK RECEIVING PROCESS
216
222
202
SOURCE
CONTROL
NETWORK SENDING PROCESS
214
CONTENT CREATION PROCESS
212
200

FIG. 2

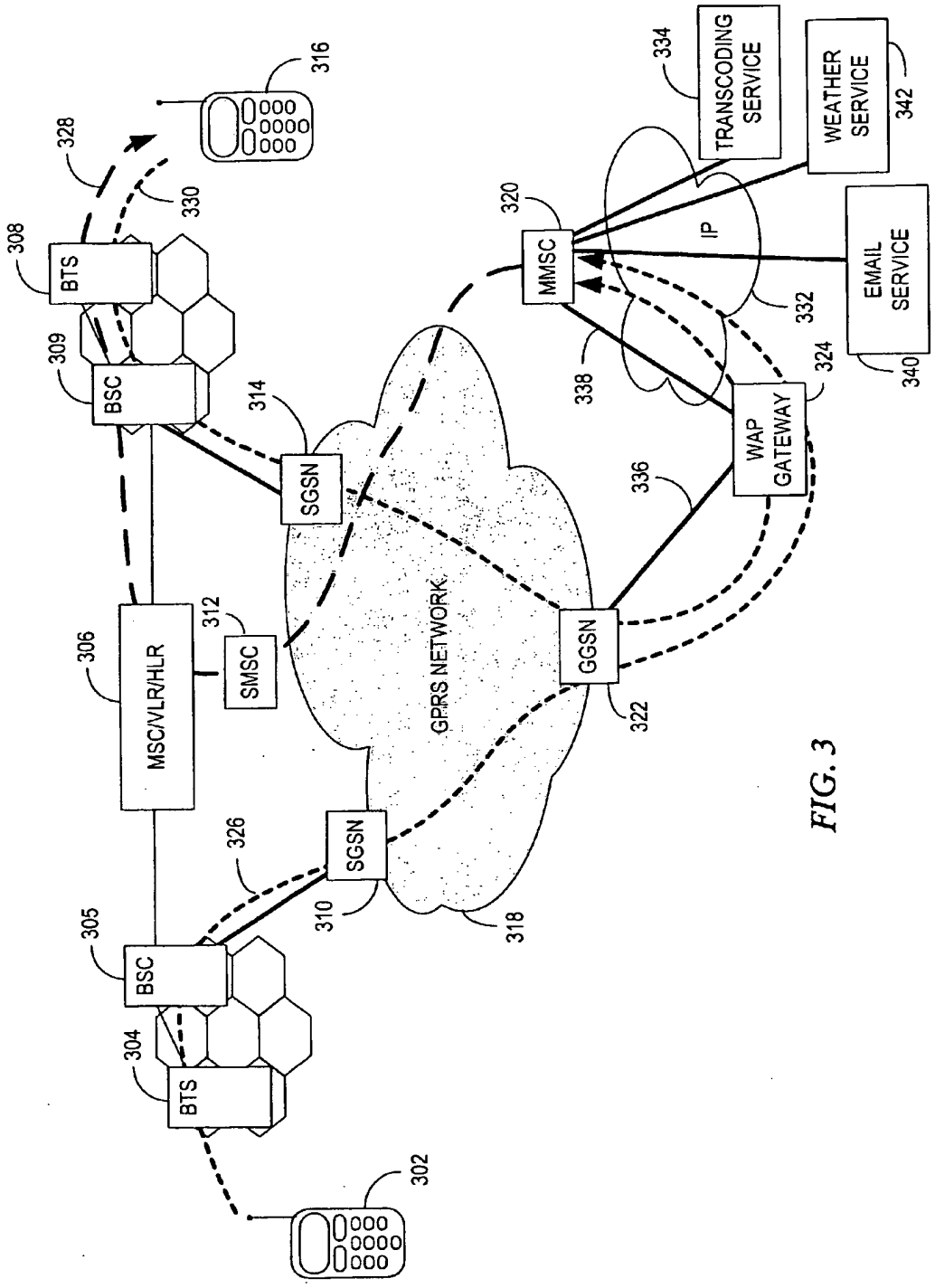

316
328
330
308
BTS
309
BSC
314
SGSN
306
MSC/VLR/HLR
312
SMSC
GPRS NETWORK
326
SGSN
310
318
305
BSC
304
BTS
302
320
MMSC
IP
334
TRANSCODING SERVICE
WEATHER SERVICE
342
EMAIL SERVICE
340
332
338
324
WAP GATEWAY
336
GGSN
322

FIG. 3

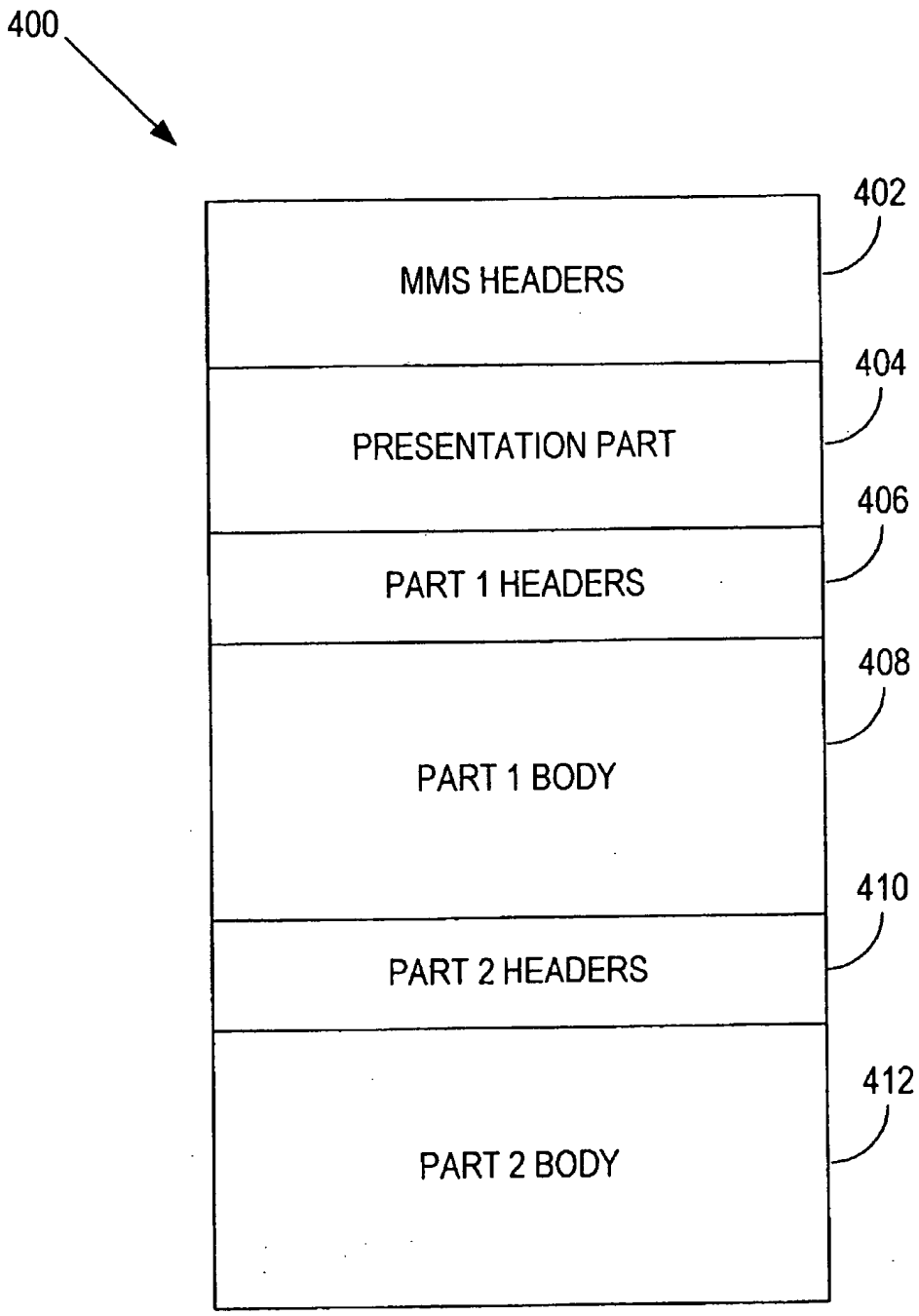

400
MMS HEADERS
402
PRESENTATION PART
404
PART 1 HEADERS
406
PART 1 BODY
408
PART 2 HEADERS
410
PART 2 BODY
412

FIG. 4

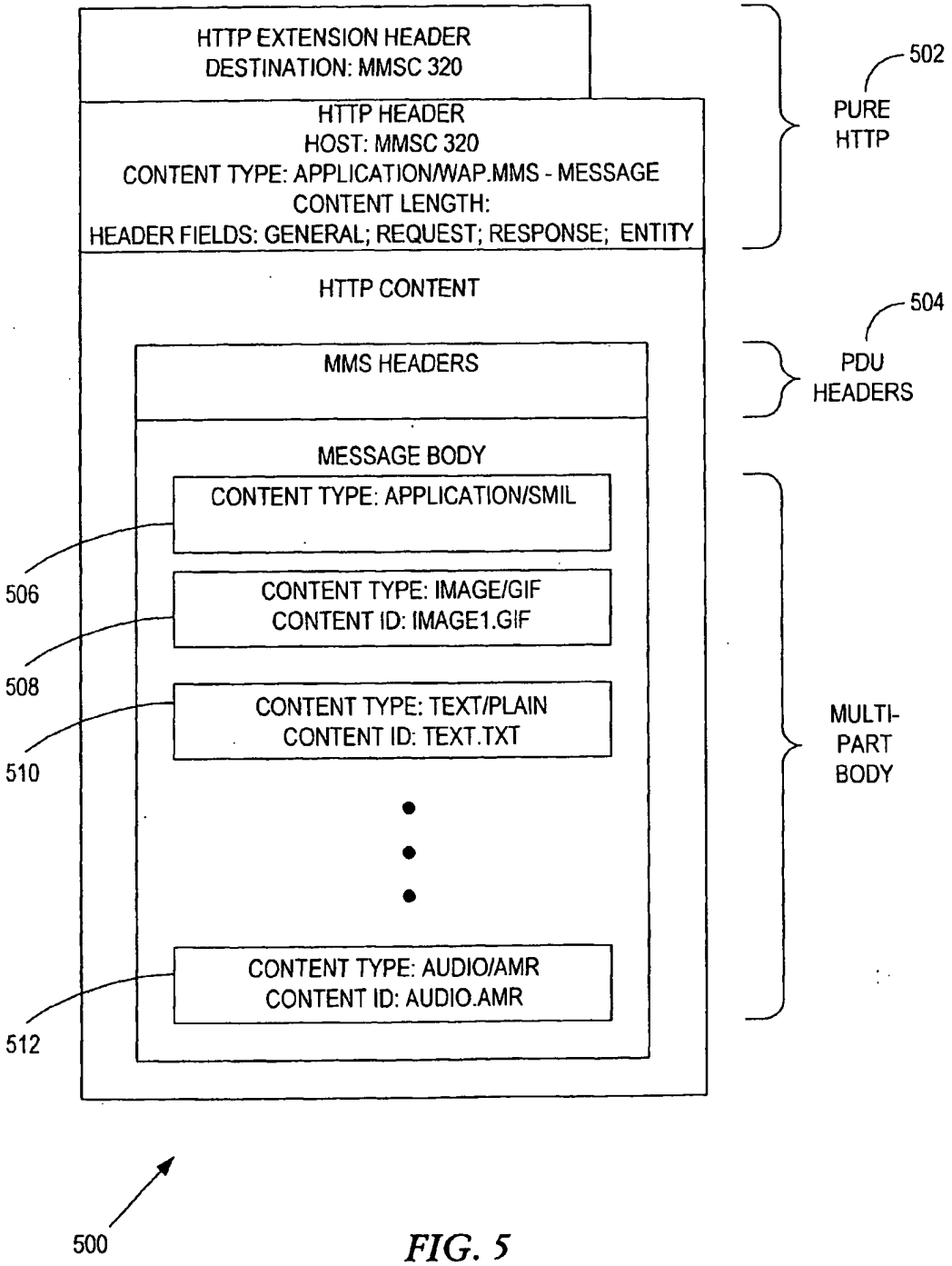

HTTP EXTENSION HEADER
DESTINATION: MMSC 320
HTTP HEADER
HOST: MMSC 320
CONTENT TYPE: APPLICATION/WAP.MMS - MESSAGE
CONTENT LENGTH:
HEADER FIELDS: GENERAL; REQUEST; RESPONSE; ENTITY
502
PURE HTTP
HTTP CONTENT
504
MMS HEADERS
PDU HEADERS
MESSAGE BODY
CONTENT TYPE: APPLICATION/SMIL
506
CONTENT TYPE: IMAGE/GIF
CONTENT ID: IMAGE1.GIF
508
CONTENT TYPE: TEXT/PLAIN
CONTENT ID: TEXT.TXT
510
MULTI-PART BODY
CONTENT TYPE: AUDIO/AMR
CONTENT ID: AUDIO.AMR
512
500

FIG. 5

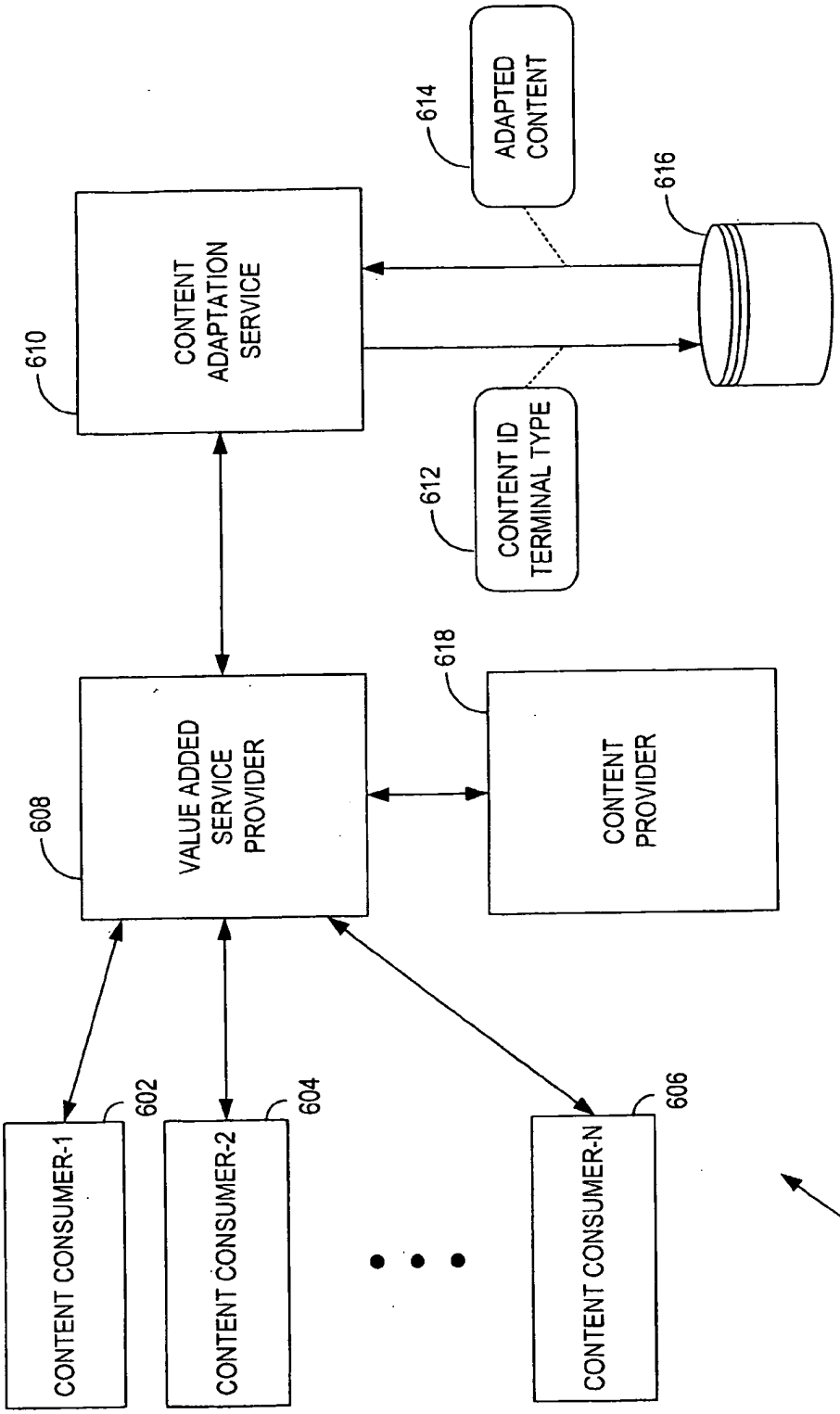

CONTENT CONSUMER-1
602
CONTENT CONSUMER-2
604
CONTENT CONSUMER-N
606
600
VALUE ADDED SERVICE PROVIDER
608
CONTENT PROVIDER
618
CONTENT ADAPTATION SERVICE
610
ADAPTED CONTENT
614
616
CONTENT ID TERMINAL TYPE
612

FIG. 6

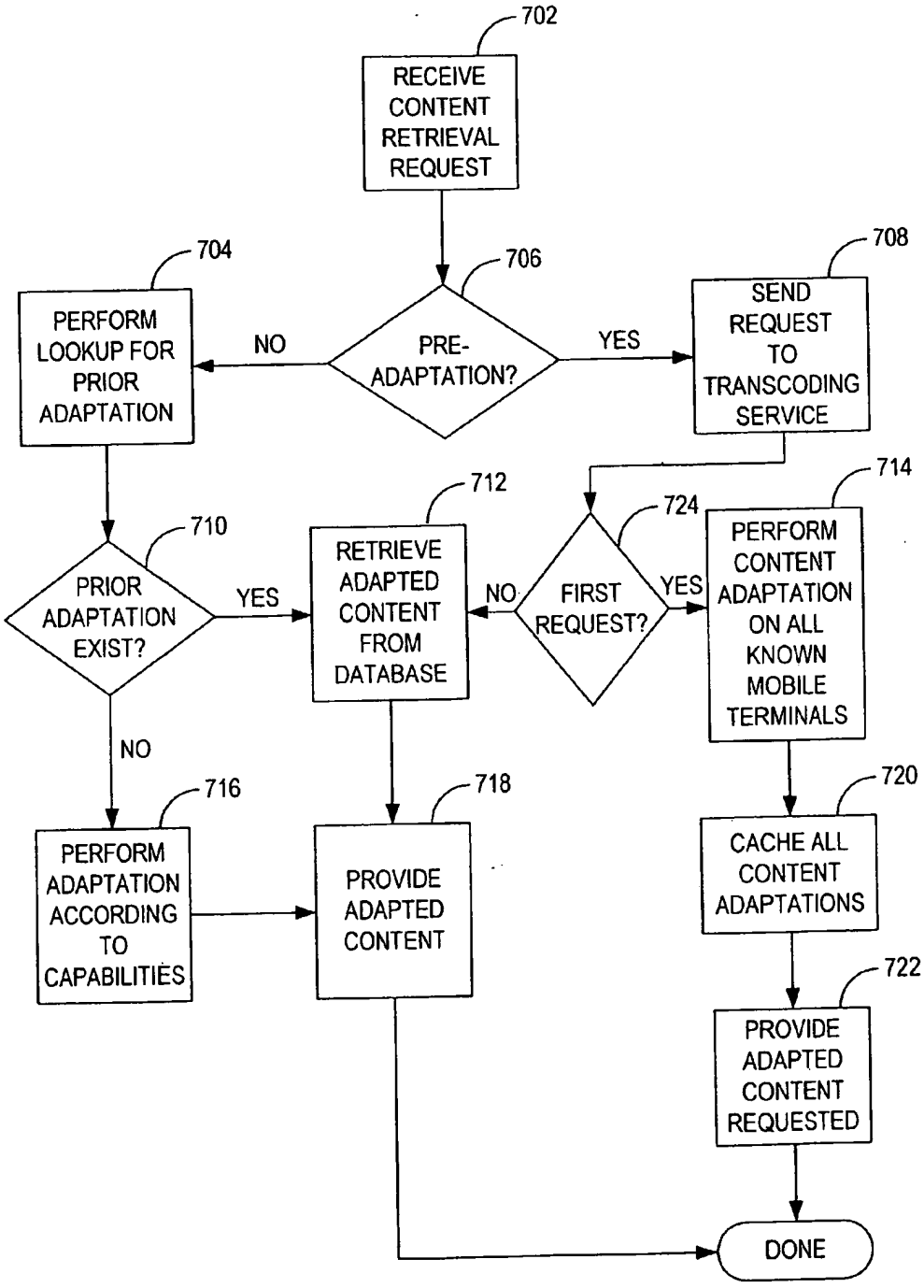

702
RECEIVE CONTENT RETRIEVAL REQUEST
704
PERFORM LOOKUP FOR PRIOR ADAPTATION
706
PRE-ADAPTATION?
NO
YES
708
SEND REQUEST TO TRANSCODING SERVICE
710
PRIOR ADAPTATION EXIST?
YES
NO
712
RETRIEVE ADAPTED CONTENT FROM DATABASE
724
FIRST REQUEST?
NO
YES
714
PERFORM CONTENT ADAPTATION ON ALL KNOWN MOBILE TERMINALS
716
PERFORM ADAPTATION ACCORDING TO CAPABILITIES
718
PROVIDE ADAPTED CONTENT
720
CACHE ALL CONTENT ADAPTATIONS
722
PROVIDE ADAPTED CONTENT REQUESTED
DONE

FIG. 7

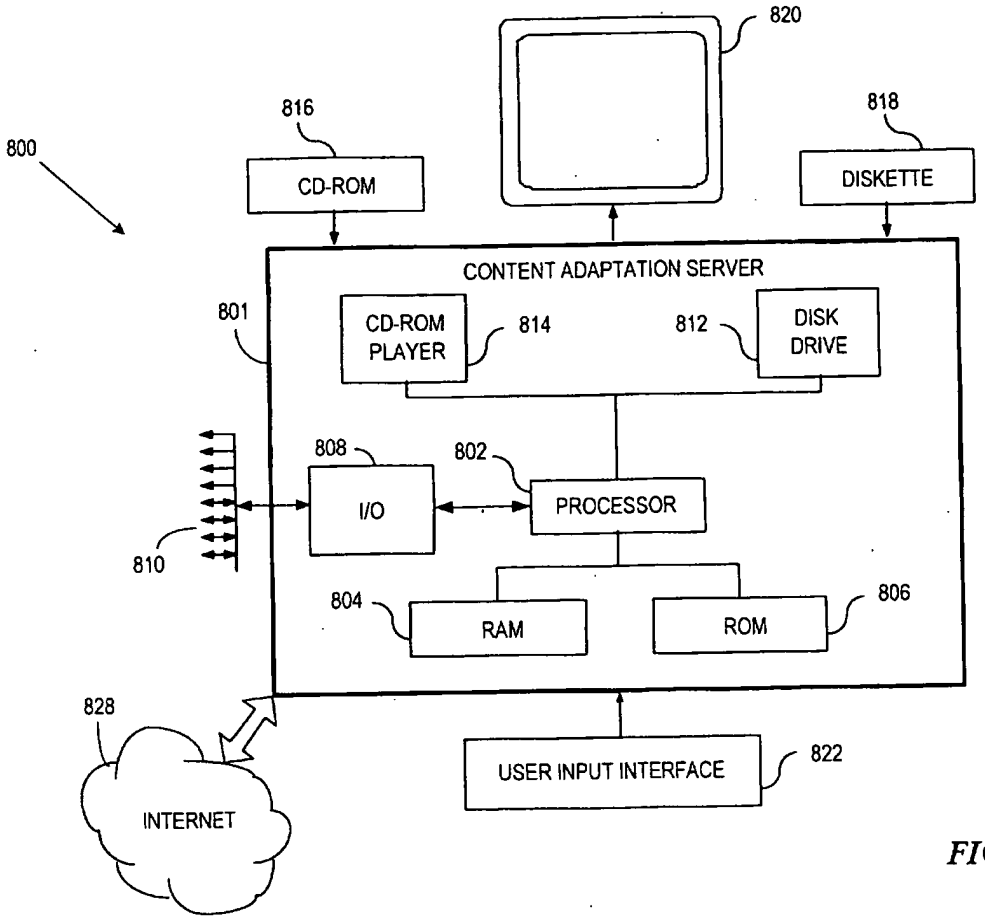

820
816
818
800
CD-ROM
DISKETTE
CONTENT ADAPTATION SERVER
801
CD-ROM PLAYER
814
812
DISK DRIVE
808
802
I/O
PROCESSOR
810
804
RAM
ROM
806
828
USER INPUT INTERFACE
822
INTERNET

FIG. 8

SYSTEM AND METHOD FOR EFFICIENT ADAPTATION OF MULTIMEDIA MESSAGE CONTENT

FIELD OF THE INVENTION

[0001] This invention relates in general to content adaptation, and more particularly, to efficient content adaptation for multimedia messages subject to repeated or mass distribution.

BACKGROUND OF THE INVENTION

[0002] The launching of the Short Message Service (SMS) has evolved into one of the most successful data services available, and the Multimedia Messaging Service (MMS) is an evolutionary step from SMS that is poised to enjoy equivalent success. Whereas pre-MMS technologies such as SMS and Enhanced Messaging Service (EMS) are limited to the transfer of content such as text, ringing tones, and monochrome bitmap pictures, MMS provides the opportunity to utilize a wide variety of rich content types such as color pictures, audio, music and video clips. MMS is based upon a store and forward model, whereby content is first transferred from one network node to a storage location, with subsequent delivery made to another network node. When the receiving terminal has comparable capabilities and resources with respect to those of the transmitting terminal, content transfer occurs normally without the need for any further consideration of the content's format. If the capabilities and resources between such endpoints are not compatible however, content adaptation becomes an important consideration.

[0003] Content adaptation generally refers to the manipulation of content to make the content suitable for specific machines, devices, and applications. Content formatted in accordance with common content formats is a desirable solution, however, market segmentation, equipment capability variation, and the unavoidable introduction of new formats are all true obstacles of interoperability. Generally, a content format refers to a convention of packaging content, where agreement on the format is required in order to build the necessary interoperability between various machines, devices, and applications. Given the limitations of the processing environment within mobile terminals, it is desirable that a reasonably small set of content formats be supported within mobile network offerings. Examples of content where agreement on format is desirable resides in the areas of audio, still images, vector graphics, video and general purpose documents.

[0004] Content adaptation may be required, for example, where content generated by one device, i.e., the content source, cannot be delivered to a destination device, i.e., the content sink, in a usable format. In such a case, the content must be made to conform to the constraints of both the delivery network and the content sink, while maintaining the content in a recognizable form. Content requiring adaptation may include an image that exceeds the memory constraints of the destination device, in which case the image may be adapted, e.g., reduced in size, such that the adapted image would fall under the size limit imposed by the destination unit. Another form of content adaptation may be required, for example, when a browser has requested a Uniform Resource Locator (URL) that references Synchronized Multimedia Integration Language (SMIL) content, but the device does not support SMIL content. In this case, for example, the SMIL layout may be converted to an alternative, although not necessarily equivalent scheme, e.g., eXtensible Hypertext Markup Language (XHTML). Still another form of content adaptation may be necessary when a user wishes to receive instant messages sent using the Session Initiation Protocol (SIP) as MMS messages on their mobile terminal. In this case, the instant message would need to be re-packaged using the MMS format. A variety of other situations in which content adaptations may be necessary and/or beneficial can similarly be envisioned.

[0005] Currently, rudimentary support for content adaptation for multimedia messages exists, such that content is adapted to support the particular characteristics of a certain mobile terminal. The content adaptation is performed based upon User Agent Profile (UAProf) attributes, which are signaled to the Multimedia Messaging Service Center (MMSC) during a retrieval transaction. Individual content adaptation, however, has a very heavy impact upon throughput and capacity and its use should be minimized so that the amount of hardware a service provider has to invest is kept at a minimum level.

[0006] Additionally, multiple requests for the same adapted content may be received, such that for each request, a separate adaptation of content is generated for each retrieval transaction. However, performing duplicative content adaptation for each retrieval transaction results in redundant operations that unnecessarily consume network resources.

[0007] Accordingly, there is a need in the communications industry for a system and method that facilitates repeated and/or mass distribution of multimedia messages containing adapted content, such that network efficiency is maximized. The present invention fulfills these and other needs, and offers other advantages over the prior art, by providing a system and method for storing content adaptations for subsequent reuse when content is requested by network elements that are compatible with the adapted content.

SUMMARY OF THE INVENTION

[0008] To overcome limitations in the prior art, and to overcome other limitations that will become apparent upon reading and understanding the present specification, the present invention discloses a system and method for storing and reusing adapted content to maximize the efficiency of distributing the content.

[0009] In accordance with one embodiment of the invention, a content adaptation system is provided to adapt content for a plurality of content consumers having varying capabilities. The content adaptation system includes a capabilities service to receive content requests from the plurality of content consumers and to retrieve their respective capabilities, a content adaptation service to provide content adaptations in accordance with the content consumer capabilities, and a database to store the content adaptations. The content adaptations may thus be reused by content consumers having substantially equivalent capabilities.

[0010] In accordance with another embodiment of the invention, a server used to facilitate content adaptations on a network is provided. The server is configured to receive a

first content request and capabilities associated with the first content request. The server is configured to provide adapted content in response to the first content request, where the adaptation of content is performed in accordance with the received capabilities. The server is further configured to reuse the adapted content for a second content request having substantially equivalent capabilities as compared to the first content request.

[0011] In accordance with another embodiment of the invention, a computer-readable medium is provided having instructions stored thereon which are executable by a content adaptation server for facilitating content adaptation by performing steps including receiving a content retrieval request and its associated capability, performing a lookup function to determine availability of previously adapted content that is compatible with the associated capability, and providing the previously adapted content in response to the content retrieval request.

[0012] In accordance with another embodiment of the invention, a method for providing adapted content is provided. The method includes receiving capability characteristics of a content requester, and locating previously adapted content relating to capability characteristics of previous content requesters. The previously adapted content is transmitted to the content requester when the capability characteristics of the content requestor substantially match the capability characteristics of the previous content requestors.

[0013] These and various other advantages and features of novelty which characterize the invention are pointed out with greater particularity in the claims annexed hereto and form a part hereof. However, for a better understanding of the invention, its advantages, and the objects obtained by its use, reference should be made to the drawings which form a further part hereof, and to accompanying descriptive matter, in which there are illustrated and described specific examples of an apparatus in accordance with the invention.

BRIEF DESCRIPTION OF THE DRAWINGS

[0014] The invention is described in connection with the embodiments illustrated in the following diagrams.

[0015] **FIG. 1** illustrates a representative networking environment in which the principles of the present invention may be applied;

[0016] **FIG. 2** is an exemplary content adaptation functional block diagram;

[0017] **FIG. 3** is a representative system level implementation of multimedia messaging and related content adaptation in accordance with the present invention;

[0018] **FIG. 4** illustrates a representative structure of an Multimedia Messaging Service (MMS) Protocol Data Unit (PDU);

[0019] **FIG. 5** illustrates a HyperText Transfer Protocol (HTTP) post request encapsulation;

[0020] **FIG. 6** illustrates a functional block diagram of a content adaptation system according to one embodiment of the present invention;

[0021] **FIG. 7** illustrates an exemplary flow diagram of a method according to one embodiment of the present invention; and

[0022] **FIG. 8** illustrates a representative computing arrangement suitable for performing content adaptation activity according to the present invention.

DETAILED DESCRIPTION OF THE INVENTION

[0023] In the following description of the exemplary embodiment, reference is made to the accompanying drawings which form a part hereof, and in which is shown by way of illustration various embodiments in which the invention may be practiced. It is to be understood that other embodiments may be utilized, as structural and operational changes may be made without departing from the scope of the present invention.

[0024] Generally, the present invention is directed to a method and system that provides previously adapted content to requesting network devices. The requesting network device capabilities are compared to previous requesting network device capabilities, such that if a capability match is found, previously adapted content may be transmitted to the requesting network device, obviating the need for an additional adaptation. In another embodiment, a pre-adaptation method is employed, whereby content adaptations for all known network device capabilities are cached or otherwise stored for future use.

[0025] **FIG. 1** illustrates a typical networking environment in which content generated by one network element is subsequently proliferated throughout other parts of the network. One aspect of the present invention is to provide a manner for facilitating seamless interaction between the various network elements when content is shared between them. In particular, the complexities involved with the content adaptations required to sustain content compliance with the various network elements are to be masked from the user.

[0026] Due to the diversity of mobile terminal capabilities and access methods, instances will arise where content **104**, generated by workstation **102**, is undeliverable to mobile terminals **116-122**, at least in a usable format. In such instances, content **104** may be transmitted to gateway **106** for intermediate storage. Content **104** may include a multitude of content types including, for example, still image graphic data, audio, music and video clips, etc. Although content **104** may be intended for all recipients **116-122**, a lack of compatibility with the content, or the method of access to the content, may prevent one or more of mobile terminals **116-122** from appropriately receiving the content.

[0027] Content **104** may represent, for example, a graphical image requiring storage capacity that exceeds the capacity of mobile terminals **116-118**. In such an instance, content adaptation-A **112** may represent a reduction in quality of the graphical image, thus reducing the storage requirements imposed by the image and allowing mobile terminals **116-118** to receive the image in its lower resolution form, e.g., content adaptation-A **112**. Network element **108** may receive content **104** via gateway **106** (or directly), and according to the principles of the present invention cause a content adaptation resulting in a reduction in quality of content **104** to yield content adaptation-A **112**. In such an instance, a single content adaptation is required to service the content retrieval sessions performed by mobile terminals **116-118**.

[0028] Content **104** may represent, on the other hand, a graphical image whose resolution requires a video display that exceeds the capacity of mobile terminals **120-122**. In such an instance, content adaptation-B **114** may represent a reduction in resolution of the graphical image, thus reducing the size of the image and allowing mobile terminals **120-122** to receive the image in its lower resolution form, e.g., content adaptation-B **114**. Network element **110** may receive content **104** via gateway **106** and according to the principles of the present invention, cause a content adaptation resulting in a reduction in resolution of content **104** to yield content adaptation-B **114**. In such an instance, a single content adaptation is required to service the content retrieval sessions performed by mobile terminals **120-122**.

[0029] Network elements **108** and **110** may be generalized as, for example, Wireless Application Protocol (WAP)/Web proxies that are capable of performing content adaptation as required by mobile terminals **116-122**. Not only are network elements **108** and **110** capable of caching or otherwise storing content **104**, but they are also able to cache/store (hereinafter "cache") the various adaptations of content **104**, e.g., content adaptation-A **112** and content adaptation-B **114**. Having the cached versions of the adapted content available, network elements **108** and **110** merely require the terminal type of mobile terminals **116-122** so that the appropriate link to content adaptations-A **112** or -B **114** may be obtained during the respective retrieval sessions by the mobile terminals.

[0030] **FIG. 2** illustrates an exemplary content adaptation functional block diagram **200** using an intermediary network component. Source node **202** illustrates a functional process that creates content for dissemination throughout the network through the use of content creation process **212**. Network sending process **214** forwards the created content to intermediary network node **204** to be received by network receiving process **216**. Content processing **218** performs content adaptation, content caching, and retrieval request processing as required, in accordance with one embodiment of the invention. Content processing **218** provides content adaptation for multiple network sink types, e.g., Sink-1 **206**, Sink-2 **208**, and Sink-N **210**. As content retrieval requests are received from network sink elements **206-210**, content processing **218** determines the requestor type and ascertains the existence of a cached version of the content requested that is compatible with requesting network sink elements **206-210**. Receiving elements **206-210** and the transport protocols (e.g. **224-228**) that deliver the content, support certain capabilities such as maximum size or resolution. The process of adaptation modifies the content to ensure that it conforms to both the sink and transport capabilities, so that the end user is at least able to receive an adapted copy of the content, rather than be denied the content altogether due to size or resolution constraints.

[0031] Sink-1 **206** through sink-N **210** represents any number of types of network elements from mobile terminals to various internet applications that provide varying degrees of access to the MMS (or other) content. Intermediary **204** represents the network element that performs Multimedia Message Adaptation (MMA) to seamlessly link the content offered by source **202** to the MMS-capable network sink devices **206-210**. Intermediary **204**, in other words, performs multimedia message adaptation to include message and media format conversion. For example, intermediary **204** may perform WAP MMS to e-mail message format conversion or may perform a Portable Network Graphics (PNG) to Joint Photographic Experts Group (JPEG) conversion and media modification. Media modification may include image scaling or file size reduction to match the MMS characteristics of sink devices **206-210**. It should be noted that while the present invention is applicable to any content and network delivery service, various aspects of the invention are described herein in terms of MMS messaging and its supported content for purposes of illustration and to facilitate an understanding of the invention.

[0032] One advantage of the present invention is the ability of intermediary **204** to provide mass delivery of adapted content to a wide variety of sink devices, especially to those sink devices comprising mobile terminals. More particularly, mobile terminals each have their own set of capabilities which limits the particular content that may be received and subsequently consumed. Capabilities such as display size, color or gray scale display, processing power, support of content formats, available memory for message storage, and regional differences of the mobile terminals may be of importance when providing adapted content to such mobile terminals. By caching the adapted content for the various capabilities, an efficient mass delivery of content may be realized.

[0033] MMS content adaptation scenarios may include MMS to e-mail, e-mail to MMS, and Web publishing, to name only a few. MMS message to e-mail adaptation involves the conversion of the MMS message by intermediary **204** into a multi-body mail message. Intermediary **204** may also convert mobile domain formats such as Wireless Bit Map (WBMP), Wireless Markup Language (WML), and Adaptive Multi-Rate (AMR) to formats that are widely used on the Internet. E-mail to MMS adaptation involves the conversion of a multi-body e-mail message to that of a multi-part MMS message. Additionally, intermediary **204** converts the content format from one that is not supported by the mobile terminal to a format that is supported by the mobile terminal, e.g., PNG to JPEG or Graphics Interchange Format (GIF). Finally, the graphical layout is adapted to the characteristics of the mobile terminal's display by intermediary **204**.

[0034] Intermediary **204** performs adaptation on units of data referred to as Multimedia Units (MMU), each of which represents a unit of data transmitted over the network that includes one or more multimedia objects, e.g., images, audio, video, text, formatted text, layout information, etc. Encapsulation is one form of adaptation performed by intermediary **204**, where encapsulation refers to how one or more multimedia objects are packaged into one data unit ready for transmission. Encapsulation may encompass both low level binary encoding, such as Base64, and application-level protocols, such as HyperText Transfer Protocol (HTTP) or MMS. Encapsulation adaptation primarily encompasses conversion of content from one application-level protocol to another. For example, instant messages using SIP may be converted to the MMS format and vice-versa, or e-mail messages may be converted to/from MMS messages. Encapsulation generally refers to the process of repackaging an MMU without altering any of the content, where a single MMU may be split into a sequence of several MMUs. For example, a long e-mail incident upon an SMS gateway may be split into several SMS messages.

Conversely, some technologies may require several MMUs to be combined, where for example, text and images from a Web page are combined into a single MMU.

[0035] Intermediary **204** may also perform size adaptation, where the number of bytes in an MMU is constrained either by agreement or by device capabilities. Network constraints encompass not only restrictions on the size of the MMU, but also restrictions on bandwidth and transmission time or latency. Although a bandwidth limit exists, e.g., General Packet Radio Service (GPRS) limits bandwidth to 21.4 kilobits per second (Kbps), the actual bandwidth is often lower and varied with time due to network congestion. For example, video originally streamed at 128 Kbps must be reduced in size, resolution, etc., in order to be transmitted real-time over a 56 Kbps connection. Further, if part of the 56 Kbps connection is suddenly reserved for another purpose, then the video size limit drops even further from 56 Kbps to something less.

[0036] Size adaptation may be achieved in several different ways. First, parts of the MMU may be removed in order to comply with the size constraint. Eliminating part of the MMU, however, results in a loss of content such that the sink network element does not receive the same content emitted by the source network element. Certain technologies may mitigate the loss of content to some extent, by designating which part of the MMU is least important.

[0037] Second, changing the encapsulation may allow size constraints to be met. For example, if the size limit is due to the transport layer or service protocol, splitting the MMU into several smaller MMUs may be acceptable. Splitting of MMUs, however, may not be acceptable where the limitations of the sink network element causes the size limitation.

[0038] Third, format conversion may result in the required size reduction. For example, the JPEG format tends to be optimized to natural scenes, e.g., photographs, and the GIF format tends to be suited to computer graphics. In cases where the current format is not ideally suited to the media, converting it to the optimal format may achieve size reduction.

[0039] Fourth, size reduction may be achieved through appearance adaptation, where for example, exactly how the appearance needs to be changed depends upon the content type. Audio content, for example, may require a change in the sampling rate; images may require a change in resolution; and video may require a change in resolution or frame rate. Appearance adaptation is generally motivated by the need to ensure compliance with the capabilities of the receiving device and are thus buried within the encoded content, masked from the underlying network.

[0040] Finally, size reduction may be achieved through altering internal media characteristics. In the case of an image, this may mean reducing the quality of the image or the number of colors it contains. In the case of audio, a bit rate alteration may be required. Generally, subtle size reductions are unlikely to be noticeable to the receiving user, especially if one or more techniques are employed to achieve the least amount of degradation in the received content.

[0041] MMS is based on a store and forward model, whereby the content source is forwarded to the content sink via, for example, a GPRS network as illustrated in **FIG. 3**.

FIG. 3 is a diagram illustrating an exemplary embodiment of a system-level implementation of multimedia messaging and related content adaptation. GPRS is a packet-switched service for Global System for Mobile Communications (GSM) that mirrors the Internet model and enables seamless transition towards 3G (third generation) networks. GPRS thus provides actual packet radio access for mobile GSM and time-division multiple access (TDMA) users, and is ideal for Wireless Application Protocol (WAP) services. While the exemplary embodiments of **FIG. 3** are generally described in connection with GPRS/GSM, it should be recognized that the specific references to GSM and GPRS are provided to facilitate an understanding of the invention. As will be readily apparent to those skilled in the art from the description provided herein, the invention is equally applicable to other technologies, including other circuit-switched and packet-switched technologies, 3G technologies, and beyond.

[0042] Referring to **FIG. 3**, mobile terminals **302** and **316** communicate with Base Transceiver Station (BTS) **304** and **308**, respectively, via an air interface. BTS **304** and **308** are components of the wireless network access infrastructure that terminates the air interface over which subscriber traffic is communicated to and from mobile terminals **302** and **316**. Base Station Controller (BSC) **305** and **309** are switching modules that provide, among other things, handoff functions, and power level control in each BTS **304** and **308**, respectively. BSC **305** and **309** controls the interface between a Mobile Switching Center (MSC) **306** and BTS **304** and **308**, and thus controls one or more BTSs in the call set-up functions, signaling, and in the use of radio channels. BSC **305** and **309** also controls the respective interfaces between Serving GPRS Support Node (SGSN) **310** and BTS **304** and SGSN **314** and BTS **308**.

[0043] SGSN **310** serves a GPRS mobile terminal by sending or receiving packets via a Base Station Subsystem (BSS), and more particularly via BSC **305** and **309** in the context of GSM systems. SGSN **310** and **314** are responsible for the delivery of data packets to and from mobile terminals **302** and **316**, respectively, within the service area, and performs packet routing and transfer, mobility management, logical link management, authentication, charging functions, etc. In the exemplary GPRS embodiment shown in **FIG. 3**, the location register of SGSN **310** stores location information such as the current cell and Visiting Location Register (VLR) associated with mobile terminal **302**, as well as user profiles such as the International Mobile Subscriber Identity Number (IMSI) of all GPRS users registered with SGSN **310**. SGSN **314** performs similar functions relating to mobile terminal **316**. SGSN **310** and **314** are ultimately coupled to SMSC **312** and/or MMSC **320** in connection with the presently described embodiment. While GSM forms the underlying technology, SGSN **310** and **314** described above are network elements introduced through GPRS technology. Another network element introduced in the GPRS context is the Gateway GPRS Support Node (GGSN) **322**, which acts as a gateway between the GPRS network **318** and WAP gateway **324**.

[0044] MMSC **320** provides messaging capabilities for the delivery of multimedia messages composed of text, photographs, video, and other media types. The messaging capabilities include mobile originated messages sent to other mobile terminals or applications and application originated

messages sent to mobile terminals or other applications. MMSC **320** is responsible for storing incoming and outgoing MMS messages, as well as the transfer of messages between different messaging systems, e.g., e-mail service **340**. In addition, MMSC **320** may provide an External Application Interface (EAIF) (not shown) that allows application developers and service providers to connect to MMSC **320** to offer value added services to mobile subscribers, such as transcoding service **334** and weather service **342**.

[0045] With the aforementioned network system described as a representative network environment, a store and forward messaging scenario is now described in which a WAP Push Framework is utilized. Dashed line **326** represents the source multimedia message from mobile terminal **302**, which is ultimately posted to MMSC **320**. The WAP protocol suite is used as the data transport mechanism because WAP provides data transport services that are optimized for mobile networks. WAP also provides uniform transport services regardless of the underlying network.

[0046] In particular, the Wireless Session Protocol (WSP) layer supplies the basis of the transport mechanism. **FIG. 4** illustrates an exemplary MMS Protocol Data Unit (PDU) **400** that may be supplied by mobile terminal **302** during a posting of content to MMSC **320**. MMS Headers **402** mainly contain information as to how to transfer the PDU from the originator, e.g. mobile terminal **302**, to the destination, e.g. mobile terminal **316**. The information may contain such information as source unit identification, sink unit identification, message identification, content type, etc. Presentation part **404** is an optional component of PDU **400** that contains information as to how the content contained within PDU **400** should be rendered onto Input/Output (I/O) of the destination device, e.g. display, speakers, tactile feedback, etc. Part 1 headers **406** and Part 2 headers **410** contain, for example, content indicators that indicate the type of content contained by Part 1 body **408** and Part 2 body **412**, respectively. The content type may be any content type supported by MMS such as images, or video, e.g., JPEG or GIF format; and text, e.g. plain or formatted text, to name only a few. Part 1 and Part 2 headers, **406** and **410** respectively, may also contain the location of the content in terms of its file name, e.g. image jpeg or text.plain.

[0047] Returning to **FIG. 3**, MMS messages are sent by mobile terminal **302** for delivery to mobile terminal **316** in, for example, an M-Send.req PDU which contains the Multipurpose Internet Mail Extensions (MIME) encapsulated MMS message content. Either the address of mobile terminal **302** or a token representing the address of mobile terminal **302** is provided within the PDU, along with the content type of the PDU. Dashed line **326** of **FIG. 3** indicates the M-Send.req PDU message flow from mobile terminal **302** to MMSC **320**. While WSP provides the wireless transport from mobile terminal **302** to WAP gateway **324**, HTTP is used to complete the post request message progression to MMSC **320**. WAP gateway **324** provides the necessary functionality required to support HTTP encapsulation as required to support multimedia messaging to MMSC **320**.

[0048] **FIG. 5** illustrates HTTP Post Request encapsulation **500** that is required to present the M-Send.req PDU received from mobile terminal **302** in WSP format to MMSC **320** in HTTP format. Pure HTTP **502** contains both the HTTP Extension Header and the HTTP Header, where the HTTP Extension Header is optional. The HTTP Extension Header may provide such information as message ID, message status, charging information (tariff classes), message recipient, message sender, message type (MMS), and MMSC version. The HTTP Header provides mandatory information such as HOST: e.g., MMSC **320**; CONTENT TYPE: e.g., MMS message; and CONTENT LENGTH: indicating the length of the multi-body part comprised of, for example, body part components **506**-**512**. In addition, the HTTP Header may contain other header fields denoted as general, request, response and entity. These additional header fields provide functionality control that is invoked by the source of the MMS message and executed by the recipient of the MMS message. Cache control may be invoked by mobile terminal **302**, for example, causing MMSC **320** to provide cache operations in response to the received MMS message.

[0049] The message body of HTTP encapsulation comprises any number of binary encoded, MIME message parts, where the content type is application/vnd.wap.mms-message. Message part **506** indicates a content type of SMIL that was generated, for example, from a URL accessed by mobile terminal **302** that further referenced SMIL content. Message part **508** indicates that a GIF image exists at location "IMAGE1.GIF", which is followed by message part **510** containing plain text at location "TEXT.TXT". Finally, the last message part **512** provides audio content from an Adaptive Multi-Rate (AMR) codec format at location "AUDIO.AMR".

[0050] Once HTTP encapsulated Post Request message **500** has been transmitted to MMSC **320** by WAP gateway **324**, an indication as to the content's receipt is provided to mobile terminal **316**, which is denoted by dashed line **328**. Notification **328** utilizes push semantics defined by the Open Mobile Alliance (OMA), which delivers a receipt notification to the receiving device, e.g., mobile terminal **316**, via for example, an SMS bearer and SMSC **312**. The MMS PDU that is used to send the notification message within the push message is M-Notification.ind. The M-Notification.ind informs mobile terminal **316** about the contents of received message **326** and its purpose is to allow mobile terminal **316** to fetch multimedia message **326** from MMSC **320**. The Notification PDU consists of MMS headers which define characteristics of the multimedia message such as: size of the multimedia message in octets; and the location of the multimedia message, e.g., MMSC **320**. Once notification message **328** has been received, a WAP/GET operation may either be automatically or manually initiated in order to receive the content specified by the URI of the notification message. Once the content has been received by mobile terminal **316**, notification to the source, e.g., mobile terminal **302**, is provided indicating successful receipt of the content.

[0051] Mobile terminal **316**, prior to performing WAP/HTTP operations with MMSC **320**, initiates a capabilities negotiation with MMSC **320**. The capabilities negotiation allows the physical characteristics of mobile terminal **316**, e.g., screen size, to be known by MMSC **320**. The capabilities are communicated according to the UAProf specification and are indicative of the MMS client's hardware, browser user-agent capabilities, network characteristics, and more. Table 1 lists an exemplary set of MMS client char-

acteristics that may be communicated during the capabilities negotiation.

TABLE 1

Attribute	Description	Sample Value
MMSMaxMessageSize	The maximum size of a multimedia message in bytes	20,480
MMSMaxImageResolution	The maximum size of an image in units of pixels	80 x 60
MMSCCPPAccept	List of supported content types conveyed as MIME types	image/JPEG audio/WAV video/MPEG text/PLAIN
MMSCCPPAcceptCharSet	List of accepted character sets that the MMS client supports	US-ASCII ISO-8859-1
MMSCCPPAcceptLanguage	List of accepted languages that the MMS client supports	English French
MMSCCPPAcceptEncoding	List of transfer encodings that the MMS client supports	base64 quoted-printable
MMSVersion	The MMS versions supported by he MMS client	2.0 1.3

[0052] Once mobile terminal **316** has initially communicated its capabilities with MMSC **320**, MMSC **320** then performs content adaptation of the content received from mobile terminal **302**, so that the content may be adequately indicated to the user of mobile terminal **316**. Alternatively, content may also be received from applications residing within IP network **332**, e.g., transcoding service **334**, weather service **342**, and e-mail service **340**, which is subsequently received and adapted by MMSC **320** for consumption by mobile terminal **316**.

[0053] One advantage offered by the present invention, is the ability of MMSC **320** to not only cache the capabilities of content consumption devices, e.g., mobile terminal **302** and **316**, but MMSC **320** may also cache the previously adapted content. In this way, content consumption devices having similar capabilities to other content consumption devices may retrieve content that has already been adapted for use by the other content consumption devices. Thus, the efficiency of the content adaptation process increases with the number of users able to use the cached, adapted content.

[0054] In order to present at least some of the advantages offered by the present invention, a temporal sequence is presented that illustrates a typical mass distributed content retrieval scenario. The users of mobile terminals **302** and **316**, for example, subscribe to a weather reporting service supplied by weather service **342**, whereby weather service **342** pushes weather information to MMSC **320** at periodic intervals. For example, weather service **342** may push weather content to MMSC **320** every morning at 8:00 am for subsequent mass delivery to all subscribers of the weather service.

[0055] The user of mobile terminal **302** is operating in a motor vehicle and is notified of the availability of weather content from MMSC **320**. Her particular mobile terminal has moderate capabilities such that she is able to retrieve and display MMS messages consisting of plain text, JPEG images having a resolution of 40x30 pixels, and a total MMS message size of 15 Kbytes. After receiving notification of the delivery of the weather content, her mobile terminal initiates a capabilities negotiation with MMSC **320** followed by an MMS retrieval request for the desired weather report.

[0056] Having the capabilities of mobile terminal **302**, MMSC **320** is able to adapt the weather content provided by weather service **342** in order to be compatible with mobile terminal **302**. In particular, weather service **342** not only provides radar graphics of the current conditions, but also offers radar projections of conditions in the future at 6 hour increments. Since retrieval of radar graphics for any future conditions would exceed the memory capability of mobile terminal **302**, MMSC **320** limits/adapts the content retrieval to include just the textual weather forecast and the current radar graphic. The adapted content is then cached into a database accessible by MMSC **320** and linked by terminal type. The content retrieval request is fulfilled by MMSC **320** by transmitting the adapted content to mobile terminal **302**, whereby the user of mobile terminal **302** is able to view the current radar view and textual weather forecast in order to plan the rest of her drive.

[0057] Shortly thereafter, mobile terminal **316** receives notification of the availability of the weather content provided by weather service **342**. After completion of the capabilities negotiation, MMSC **320** checks the database for any cached, adapted content that is linked to mobile terminals having capabilities similar to mobile terminal **316**. Since mobile terminal **316** has substantially equivalent capabilities to that of mobile terminal **302**, a match is found to the cached content. The cached content is then transmitted to mobile terminal **316** immediately, thereby obviating the need for MMSC **320** to re-adapt the content for mobile terminal **316**.

[0058] **FIG. 6** illustrates a functional block diagram of a content adaptation system according to the principles of the present invention. Content consumers **1602** through N **606** may represent any network node having the capability to browse for and retrieve content generated by content provider **618**. Value Added Service Provider (VASP) **608** receives content requests from content consumers **1602** through N **606**, negotiates their capabilities, and gathers the requested content from content provider **618**. VASP **608** also communicates with Content Adaptation Service (CAS) **610** as required in order to adapt the content requested by content consumers **1602** through N **606** to meet their respective needs. VASP **608** may also determine whether caching of adapted content is permitted, and in the affirmative case, the adapted content is cached within database **616** and indexed according to content ID and terminal type. Signaling of adapted content cache capability may be implemented, for example, using HTTP header information **502** of **FIG. 5**, in which a toggle bit may be set in the general header portion of header information **502** to indicate whether or not content caching is permitted.

[0059] In one embodiment according to the present invention, a pre-adaptation method is performed by VASP **608**. In this case, VASP **608** would, for example, correspond to transcoding service **334** of **FIG. 3**, where transcoding service **334** would have knowledge of all of the current mobile terminal types used on the market at a particular time. Once an MMS retrieve message is received by VASP **608**, then the

content pertaining to the retrieve message is extracted from content provider **618**. The content received would then undergo as many pre-adaptations as required in order to fulfill the needs of content consumers **1602** through N **606**. Each adapted content would be indexed with tag **612** whereby a content ID and a terminal type is used for future recall.

[0060] The present invention may be generalized to, for example, WAP/Web Proxies that are configured to perform content adaptation. Taking for example, WAP gateway **324** of **FIG. 3**, the VASP, content adaptation function, and database function may be incorporated there or in a Web Proxy, thus obviating the need for MMSC **320** to perform content adaptation functions. In general, the present invention is modular, whereby the functions supported by VASP **608**, content adaptation service **610**, and database **616**, for example, may be distributed in one particular implementation, and conversely co-located within a WAP Gateway, a Web Proxy, or MMSC, in another particular implementation.

[0061] **FIG. 7** illustrates an exemplary flow diagram of a method according to the present invention. Content retrieval requests are received in step **702** by, for example, VASP **608** of **FIG. 6**, WAP gateway **324** or MMSC **320** of **FIG. 3**. In a pre-adaptation mode of operation, process step **706** takes the Yes path to process step **708**. In this case, pre-adaptation is the preferred mode of content adaptation, which requires that content adaptations be provided for all known mobile terminal types and cached for later use. In such an instance, the content retrieval request is passed onto, for example, transcoding service **334** of **FIG. 3**, whereby the capabilities of all known mobile terminal types is known. For each distinct mobile terminal capability type, a content adaptation is prepared for each mobile terminal capability type in step **714**, if not already done as determined by step **724**, and subsequently cached into memory in step **720**, e.g., database **616** of **FIG. 6**. The adapted content is also provided to the requesting device for future consumption. If the adaptations have already been performed, then the adapted content is simply retrieved as in step **712** and provided in step **718**.

[0062] In an alternative embodiment, pre-adaptation is not the preferred mode of content adaptation and the No path is taken from process step **706**. In such a case, any content adaptations that have been performed in the past are analyzed in step **704** to determine whether the capabilities of the requesting mobile terminals for the past adaptations match the capabilities of the current requesting mobile terminal. If a match exists, as determined in step **710**, the Yes path to step **712** is taken. In step **712**, it has been determined that a previous content adaptation does in fact match the capabilities of the current requesting mobile terminal and the adapted content is thus fetched from cache, e.g. database **616**, and provided to the current requesting mobile terminal in step **718**. If, however, no previous content adaptations exist within database **616**, then a new content adaptation is performed in step **716**, that matches the capabilities of the current requesting mobile terminal and is subsequently provided to the current requesting mobile terminal in step **718**.

[0063] The present invention may be used to reduce the amount of overhead generated by providing individual content adaptations, through the use of previously adapted content when previously adapted content is available and usable. The present invention, therefore, allows reuse of adapted content thus increasing the efficiency of the network. In a particular example, 10,000 subscribers may have subscribed to a service that provides the latest sports reports concerning football news. Half of the subscribers each have identical MMS handsets, 20% of the subscribers have an upgraded version of the MMS handset with enhanced capabilities, and the final 30% have a mixture of MMS handsets from various vendors. In such an instance, the present invention allows for the content adaptation of the football news reports into two separate content adaptations, the first adaptation used by the 50% class of subscribers and the second adaptation being used by the 20% class of subscribers, whereby the two content adaptations would serve 70% of the subscriber base. It can be seen, therefore, that the present invention obviates the need for 7,000 independent content adaptations to be performed by first caching the results of two adaptations; and providing the cached results for future use by 70% of the compatible subscribers.

[0064] Using the description provided herein, the invention may be implemented as a machine, process, or article of manufacture by using standard programming and/or engineering techniques to produce programming software, firmware, hardware or any combination thereof. Any resulting program(s), having computer-readable program code, may be embodied on one or more computer-usable media, such as disks, optical disks, removable memory devices, semiconductor memories such as RAM, ROM, PROMS, etc. Articles of manufacture encompassing code to carry out functions associated with the present invention are intended to encompass a computer program that exists permanently or temporarily on any computer-usable medium or in any transmitting medium which transmits such a program. Transmitting mediums include, but are not limited to, transmissions via wireless/radio wave communication networks, the Internet, intranets, telephone/modem-based network communication, hard-wired/cabled communication network, satellite communication, and other stationary or mobile network systems/communication links. From the description provided herein, those skilled in the art will be readily able to combine software created as described with appropriate general purpose or special purpose computer hardware to create a content adaptation system and method in accordance with the present invention.

[0065] The network servers or other systems for providing content adaptation functions in connection with the present invention may be any type of computing device capable of processing and communicating information. The network servers utilize computing systems to control and manage the content adaptation activity. An example of a representative computing system capable of carrying out operations in accordance with the invention is illustrated in **FIG. 8**. Hardware, firmware, software or a combination thereof may be used to perform the various content adaptation functions and operations described herein. The computing structure **800** of **FIG. 8** is an example computing structure that can be used in connection with such a content adaptation system.

[0066] The example computing arrangement **800** suitable for performing the content adaptation activity in accordance with the present invention includes the content adaptation server **801**, which includes a central processor (CPU) **802** coupled to random access memory (RAM) **804** and read-only memory (ROM) **806**. The ROM **806** may also be other

types of storage media to store programs, such as programmable ROM (PROM), erasable PROM (EPROM), etc. The processor **802** may communicate with other internal and external components through input/output (I/O) circuitry **808** and bussing **810**, to provide control signals and the like. For example, MMS client capabilities such as those exemplified in Table 1 may be received by content adaptation server **801** to enable content adaptation according to the MMS client capabilities. External data storage devices, such as content adaptation databases, may be coupled to I/O circuitry **808** to facilitate lookup functions according to the present invention, to allow reuse of previously adapted content. Alternatively, such databases may be locally stored in the storage/memory of the server **801**, or otherwise accessible via a local network or networks having a more extensive reach such as the Internet **828**. The processor **802** carries out a variety of functions as is known in the art, as dictated by software and/or firmware instructions.

[0067] The content adaptation server **801** may also include one or more data storage devices, including hard and floppy disk drives **812**, CD-ROM drives **814**, and other hardware capable of reading and/or storing information such as DVD, etc. In one embodiment, software for carrying out the content adaptation operations in accordance with the present invention may be stored and distributed on a CD-ROM **816**, diskette **818** or other form of media capable of portably storing information. These storage media may be inserted into, and read by, devices such as the CD-ROM drive **814**, the disk drive **812**, etc. The software may also be transmitted to the content adaptation server **801** via data signals, such as being downloaded electronically via a network, such as the Internet. The content adaptation server **801** is coupled to a display **820**, which may be any type of known display or presentation screen, such as LCD displays, plasma display, cathode ray tubes (CRT), etc. A user input interface **822** is provided, including one or more user interface mechanisms such as a mouse, keyboard, microphone, touch pad, touch screen, voice-recognition system, etc.

[0068] The content adaptation server **801** may be coupled to other computing devices, such as the landline and/or wireless terminals via a network. The server may be part of a larger network configuration as in a global area network (GAN) such as the Internet **828**, which allows ultimate connection to the various landline and/or mobile client/watcher devices.

[0069] The foregoing description of the various embodiments of the invention has been presented for the purposes of illustration and description. It is not intended to be exhaustive or to limit the invention to the precise form disclosed. Many modifications and variations are possible in light of the above teaching. Thus, it is intended that the scope of the invention be limited not with this detailed description, but rather determined from the claims appended hereto.

What is claimed is:

1. A content adaptation system to provide adapted content to a plurality of content consumers having differing capabilities, the content adaptation system comprising:

a capabilities service coupled to receive content requests from the plurality of content consumers and to retrieve their respective capabilities;

a content adaptation service coupled to provide content adaptations in accordance with the plurality of content consumer capabilities; and

a database coupled to store the content adaptations, wherein the content adaptations are reused by content consumers having substantially equivalent capabilities.

2. The content adaptation system according to claim 1, wherein multiple content adaptations are stored based upon the capabilities of a predetermined set of content consumers.

3. The content adaptation system according to claim 2, wherein a first content request initiates the storage of the multiple content adaptations.

4. The content adaptation system according to claim 2, wherein the content adaptations stored in the database are indexed by a terminal type indicative of their corresponding capabilities.

5. The content adaptation system according to claim 4, wherein the content adaptations stored in the database are further indexed by a content identification.

6. The content adaptation system according to claim 5, wherein the content adaptation service provides the index to the database to retrieve content adaptations from the database relating to the index.

7. The content adaptation system according to claim 1, wherein a content adaptation is stored based upon the capabilities of the requesting content consumer.

8. The content adaptation system according to claim 7, wherein a content request from the requesting content customer initiates the storage of the content adaptation.

9. The content adaptation system according to claim 8, wherein the content adaptation stored in the database is indexed by a terminal type indicative of its corresponding capabilities.

10. The content adaptation system according to claim 9, wherein the content adaptation stored in the database is further indexed by a content identification.

11. The content adaptation system according to claim 10, wherein the content adaptation service provides the index to the database to retrieve the content adaptation from the database relating to the index.

12. The content adaptation system according to claim 1, wherein the capabilities service, the content adaptation service and the database are co-located.

13. The content adaptation system according to claim 12, wherein the co-location exists within a Web proxy.

14. The content adaptation system according to claim 12, wherein the co-location exists within a Wireless Application Protocol (WAP) gateway.

15. The content adaptation system according to claim 12, wherein the co-location exists within a Multimedia Messaging Service Center (MMSC).

16. The content adaptation system according to claim 1, wherein the capabilities service, the content adaptation service and the database are distributed throughout the content adaptation system.

17. A server for facilitating content adaptations on a network, comprising:

means for receiving a first content request;

means for receiving capabilities associated with the first content request;

means for providing adapted content in response to the first content request, wherein the adaptation of content is performed in accordance with the received capabilities; and

means for reusing the adapted content for a second content request having capabilities substantially corresponding to the capabilities associated with the first content request.

18. The server according to claim 17, wherein the means for reusing the adapted content comprises a database arranged to store the adapted content.

19. The server according to claim 18, wherein the database is arranged to receive an index indicative of the received capabilities.

20. The server according to claim 19, wherein the database retrieves previously adapted content in response to receiving the index.

21. A computer-readable medium having instructions stored thereon which are executable by a content adaptation server for facilitating content adaptation by performing steps comprising:

receiving a content retrieval request and its associated capability;

performing a lookup function to determine availability of previously adapted content that is compatible with the associated capability; and

providing the previously adapted content in response to the content retrieval request.

22. A method for providing adapted content, comprising:

receiving capability characteristics of a content requester;

locating previously adapted content relating to capability characteristics of previous content requestors; and

transmitting the previously adapted content to the content requester when the capability characteristics of the content requestor substantially match the capability characteristics of the previous content requestors.

23. The method according to claim 22, wherein the previously adapted content is generated based on all known capability characteristics of a predetermined set of content requesters.

24. The method according to claim 23, wherein the previously adapted content is cached.

25. The method according to claim 24, wherein the previously adapted content is retrieved from the cache based upon an index comprising a content identification and a terminal type.

26. The method according to claim 22, wherein the previously adapted content is generated based on the capability characteristics of the content requestor.

27. The method according to claim 26, wherein the previously adapted content is cached.

28. The method according to claim 27, wherein the previously adapted content is retrieved from the cache based upon an index comprising a content identification and a terminal type.

* * * * *

US007003551B2

(12) **United States Patent**
Malik

(10) **Patent No.: US 7,003,551 B2**
(45) **Date of Patent: Feb. 21, 2006**

(54) **METHOD AND APPARATUS FOR MINIMIZING STORAGE OF COMMON ATTACHMENT FILES IN AN E-MAIL COMMUNICATIONS SERVER**

(75) Inventor: **Dale W. Malik**, Dunwoody, GA (US)

(73) Assignee: **BellSouth Intellectual Property Corp.**, Wilmington, DE (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 795 days.

(21) Appl. No.: **09/725,719**

(22) Filed: **Nov. 30, 2000**

(65) **Prior Publication Data**

US 2002/0065892 A1 May 30, 2002

(51) **Int. Cl.**
G06F 15/16 (2006.01)

(52) **U.S. Cl.** **709/206**; 709/232

(58) **Field of Classification Search** 709/217, 709/206, 232, 200, 203, 226, 218, 219, 201; 370/238; 455/524; 358/402; 713/201; 705/14; 707/200, 3, 101, 204; 710/33; 715/500, 513, 826; 717/141; 379/93
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,323,394	A *	6/1994	Perlman	370/238
5,327,534	A *	7/1994	Hutchison et al.	709/226
5,379,448	A *	1/1995	Ames et al.	455/524
5,771,355	A *	6/1998	Kuzma	709/232
5,778,395	A *	7/1998	Whiting et al.	707/204
5,781,901	A	7/1998	Kuzma	707/10
5,809,481	A *	9/1998	Baron et al.	705/14
5,832,208	A *	11/1998	Chen et al.	713/201
5,892,909	A *	4/1999	Grasso et al.	709/201
5,903,723	A *	5/1999	Beck et al.	709/200
5,905,712	A *	5/1999	Cresswell et al.	370/238
5,937,160	A *	8/1999	Davis et al.	709/203
6,009,462	A *	12/1999	Birrell et al.	709/206
6,021,433	A *	2/2000	Payne et al.	709/219
6,035,104	A *	3/2000	Zahariev	709/203
6,035,121	A *	3/2000	Chiu et al.	717/141
6,073,142	A *	6/2000	Geiger et al.	715/500
6,092,101	A *	7/2000	Birrell et al.	709/206
6,138,149	A *	10/2000	Ohmura	709/218
6,199,061	B1 *	3/2001	Blewett et al.	707/3
6,246,669	B1 *	6/2001	Chevalier et al.	370/238
6,256,672	B1 *	7/2001	Redpath	709/232

(Continued)

OTHER PUBLICATIONS

vnews: a multicast, multimedia news service with virtual messagesKowalchuk, R.J.; Hilderman, R.J.; Hamilton, H.J.; Computers and Communications, 1996., Conference Proceedings of the 1996 IEEE Fifteenth Annual International Phoenix Conference on , 27-29 Ma.*

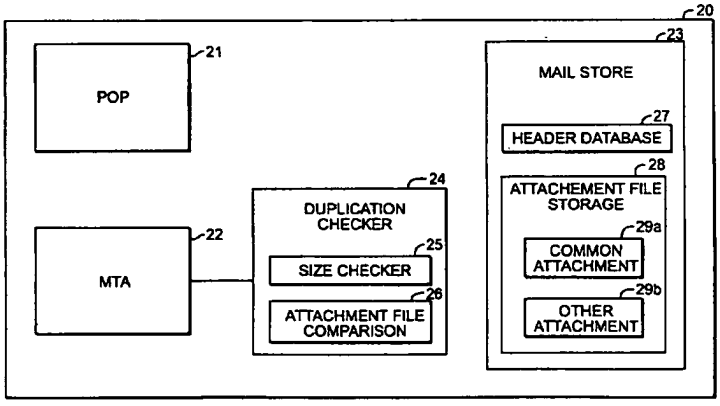
(Continued)

Primary Examiner—Thong Vu
(74) *Attorney, Agent, or Firm*—Thomas, Kayden, Horstmeyer & Risley LLP

(57) **ABSTRACT**

The present invention provides an e-mail communications system that minimizes the number of duplicate copies of common attachment files to e-mail communications that are stored in the mail store of an e-mail server. When the e-mail server receives an e-mail attachment file that is larger than a threshold size, the server performs a database search for another copy of the attachment file in the mail store. If another copy is located, the system creates a pointer in the mail store that associates the located attachment file with the e-mail for the additional recipient(s). Attachment files are deleted only after the recipients of the associated e-mail communications delete each of the respective e-mails.

13 Claims, 6 Drawing Sheets



U.S. PATENT DOCUMENTS

6,275,848	B1	8/2001	Arnold	709/206
6,275,850	B1 *	8/2001	Beyda et al.	709/206
6,278,449	B1 *	8/2001	Sugiarto et al.	715/826
6,321,242	B1 *	11/2001	Fogg et al.	715/513
6,327,594	B1 *	12/2001	Van Huben et al.	707/200
6,366,949	B1 *	4/2002	Hubert	709/206
6,405,244	B1 *	6/2002	Bando et al.	709/206
6,453,340	B1 *	9/2002	Emura	709/206
6,457,044	B1 *	9/2002	IwaZaki	709/206
6,463,430	B1 *	10/2002	Brady et al.	707/3
6,499,001	B1 *	12/2002	Meyer	702/187
6,505,236	B1 *	1/2003	Pollack	709/206
6,560,639	B1 *	5/2003	Dan et al.	709/218
6,606,654	B1 *	8/2003	Borman et al.	709/219
6,611,830	B1 *	8/2003	Shinoda et al.	707/3
6,662,212	B1 *	12/2003	Chandhok et al.	709/206
6,728,733	B1 *	4/2004	Tokui	707/200
6,728,752	B1 *	4/2004	Chen et al.	709/203
6,732,111	B1 *	5/2004	Brodersen et al.	707/101
6,738,800	B1 *	5/2004	Aquilon et al.	709/206
6,757,712	B1 *	6/2004	Bastian et al.	709/206
6,772,139	B1 *	8/2004	Smith, III	707/3
6,801,962	B1 *	10/2004	Taniguchi et al.	710/33
6,829,636	B1 *	12/2004	Kubik et al.	709/206

OTHER PUBLICATIONS

Digital toolbox. Controlling interests [MIME]; Thomas, B.; Internet Computing, IEEE , vol.: 1 , Issue: 4 , Jul.-Aug. 1997.*

Flexible Control of Downloaded Executable Content—Jaeger, Islam, Anand, Prakash, Liedtke (ResearchIndex) ; citeseer.nj.nec.com/jaeger97flexible.html.*

SiteScape for IU Faculty; www.indiana.edu/~ssf/b155.htm.*

Email Protocols : SMTP, MIME, POP & IMAP; www.opus1.com/www/presentations/emailproto.*

WPL MAC Tutorial; users.rcn.com/woblib/mactut.htm.*

Standardization of the Complement Adjunct Distinction—Adam Meyers Catherine (1994) ; nlp.cs.nyu.edu/publication/papers/adj-compl-old.ps.*

On the Semantics of 'Current-Time' In Temporal Databases—Finger (1996) ftp.ime.usp.br/pub/mfinger/SBBD96.ps.gz.*

Kerberos Authentication and Authorization System—Miller, Neuman, Schiller.. (1988) krasse.ce.chalmers.se/Security/techplan.PS.gz.*

How to Use Automatic Formatting to Turn File Names into Hyperlinks www.wellesley.edu/Computing/World/hyperlinks.html.*

Adventure Software—Internet Adventurer—File Attachments; www.inetadv.net/help/newsatt.htm.*

Microsoft Office Developer Forum—Office 97 Programmer's Guide—Microsoft Access Objects; www.microsoft.com/officedev/articles/Opg/003/003.htm.*

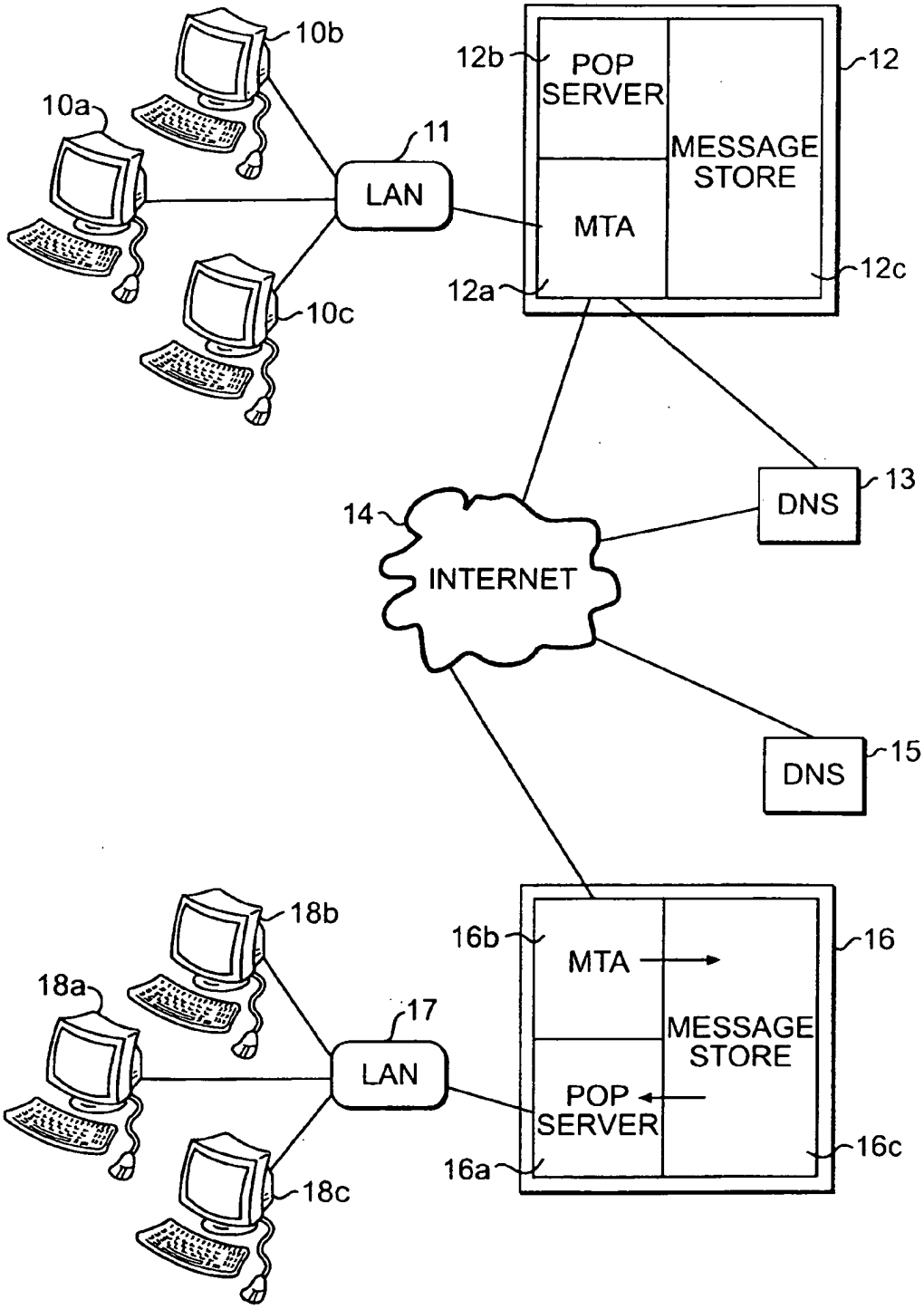
Design Specification; cs.wwc.edu/~fortsa/se/designspec.html.*

Initial Use of COTS Tools in the OBJS Virtual Office; www.objs.com/survey/Scenario-1.html.*

Modeling Mobile IP in Mobile UNITY—Peter Mccann (1998) www.cs.wustl.edu/cs/techreports/1998/wucs-98-03.ps.Z.*

* cited by examiner

FIG. 1
PRIOR ART



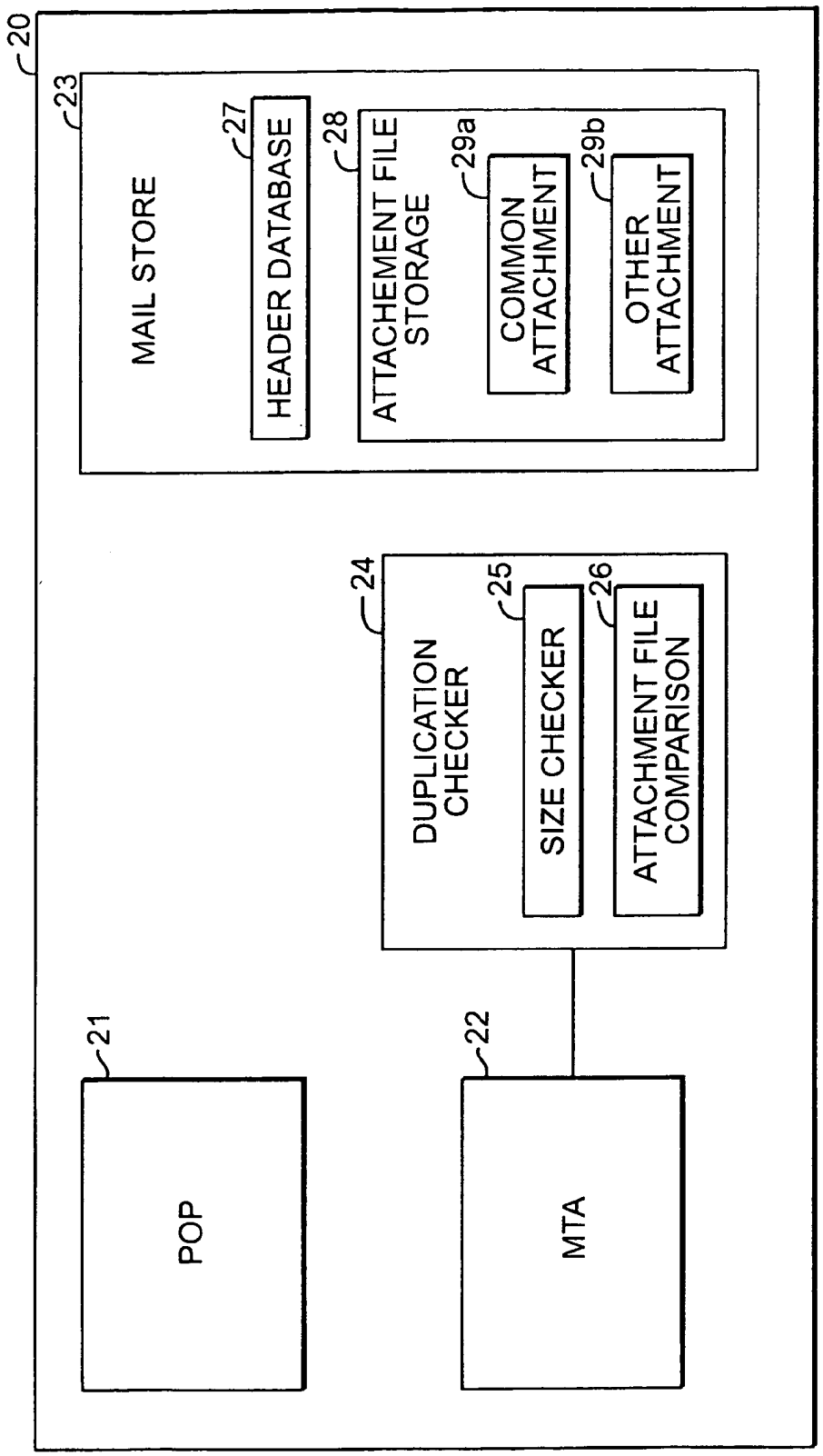

20
23
MAIL STORE
27
HEADER DATABASE
28
ATTACHEMENT FILE STORAGE
29a
COMMON ATTACHMENT
29b
OTHER ATTACHMENT
24
DUPLICATION CHECKER
25
SIZE CHECKER
26
ATTACHMENT FILE COMPARISON
21
POP
22
MTA

FIG. 2

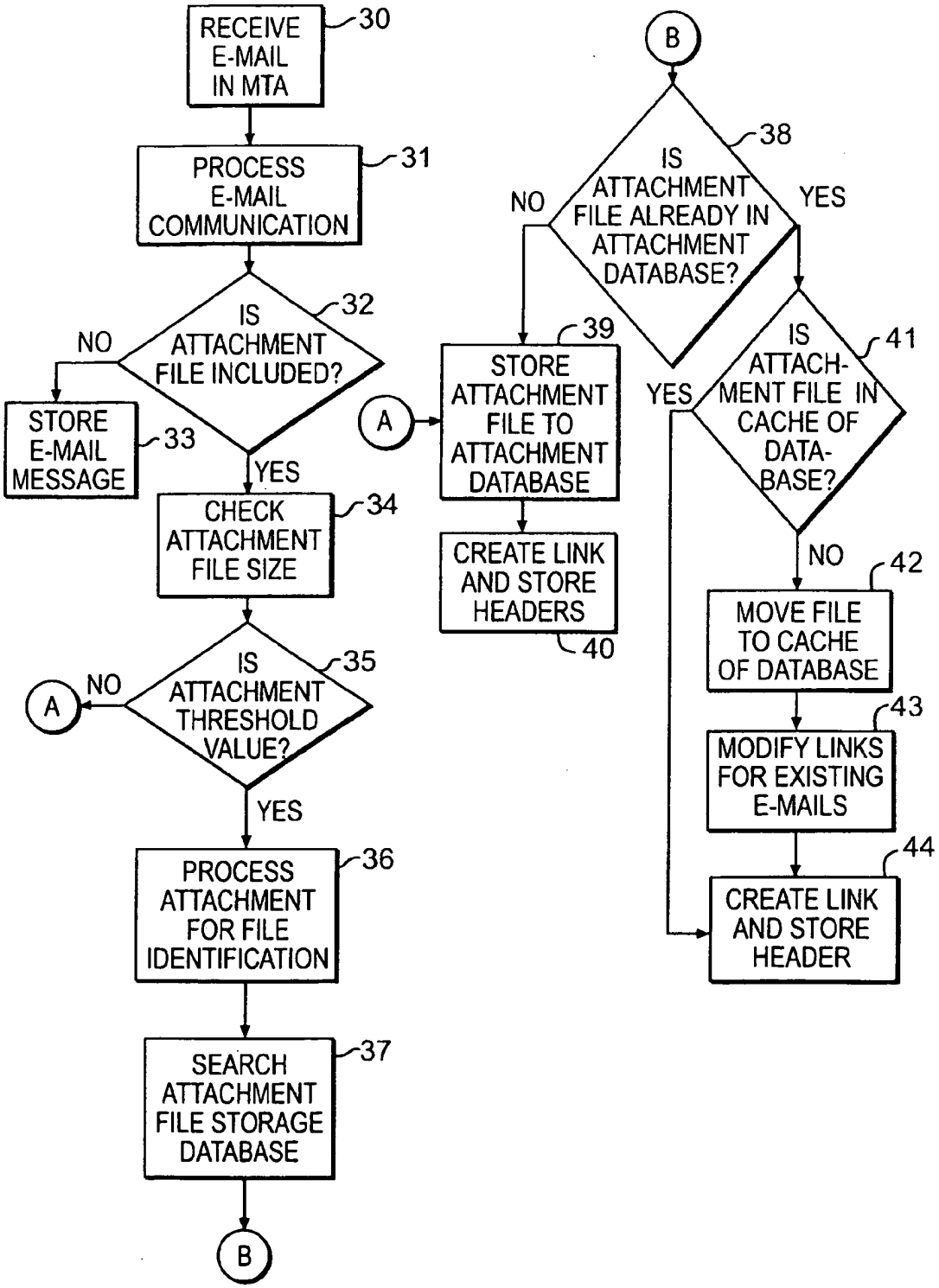

RECEIVE E-MAIL IN MTA
30
PROCESS E-MAIL COMMUNICATION
31
IS ATTACHMENT FILE INCLUDED?
32
NO
STORE E-MAIL MESSAGE
33
YES
CHECK ATTACHMENT FILE SIZE
34
IS ATTACHMENT THRESHOLD VALUE?
35
NO
A
YES
PROCESS ATTACHMENT FOR FILE IDENTIFICATION
36
SEARCH ATTACHMENT FILE STORAGE DATABASE
37
B
A
STORE ATTACHMENT FILE TO ATTACHMENT DATABASE
39
CREATE LINK AND STORE HEADERS
40
B
IS ATTACHMENT FILE ALREADY IN ATTACHMENT DATABASE?
38
NO
YES
IS ATTACH-MENT FILE IN CACHE OF DATA-BASE?
41
YES
NO
MOVE FILE TO CACHE OF DATABASE
42
MODIFY LINKS FOR EXISTING E-MAILS
43
CREATE LINK AND STORE HEADER
44

FIG. 3

HEADER DATABASE

HEADER#	USER NAME	SUBJECT	DATE RECEIVED	FROM	ATTACHMENT
1	gobi 7265	Funny Joke	10/31/00	joe@anyisp.com	✓ 3
2	mody 6380	Hysterical Email!	10/27/00	synth@izewr.com	
3	gore 7923	Political Announcement	9/9/00	clinton@pres.com	
4	welsh 9929	Final Report	3/10/00	jack@gebc.com	✓ 2
5	larry 3926	That is Really Funny	11/2/00	gobi@7265	✓ 3
6	johm 9938	Funny Joke	10/31/00	joe@anyisp.com	✓ 3
7	bear 3827	Meeting Notice	9/29/00	raph@auren.com	
8	bird 2392	Stars & Stripes	7/4/00	uncle@sam.gov	✓ 6

FIG. 4

CACHED ATTACHMENT FILE STORAGE DATABASE

HEADER #	LINK No.	FILE TYPE	TITLE	SIZE	Ms-DOS NAME	SOFTWARE	VERSION	AUTHOR	CREATION DATE	LAST MODIFIED	REVISION	PAGES	CHARTERED	DESIGN
2	1	TEXT	FUNNY JOKE	1MB	FUNNY.WPD	WORDPERFECT	6.0	JOHNSON	11/01/00	11/03/00	3	18	9273	-
4	2	TEXT	REPORT	0.MB	REPORT.DOC	WORD	99	WELCH	9/22/99	3/9/00	9	205	998625	-
1,5,6	3	VIDEO	WHASSUP	2-3 MB	WHASSUP.AU	REAL AUDIO	2.0	SPIKE	10/6/00	10/6/00	-	-	-	-
11	4	PRE-SENT-ATION	DC	5MB	DCPRESNT.PWR	POWERPOINT	98	WILLIAM	9/9/99	-	-	-	-	SLIDES

MAIN ATTACHMENT FILE STORAGE DATABASE

HEADER #	LINK No.	FILE TYPE	TITLE	SIZE	Ms-DOS NAME	SOFTWARE	VERSION	AUTHOR	CREATION DATE	LAST MODIFIED	REVISION	PAGES	CHARTERED	DESIGN
10	VIDEO	EXER-CISE VIDEO	EXERCISE .AV	2MB	EXERCISE.QV	WINDOWS MEDIA PLAYER	98	MIKE	-	-	-	-	-	-
8	MUSIC	STARS & STRIPES	STSTR.AV	1MB	STSTR. AV	REAL AUDIO	2	-	-	-	-	-	-	-
16	TAX	HELLO	LETTER .DOC	0.2MB	LETTER.DOC	WORD	98	BIRD	9/8/99	10/9/00	16	3	987	-

FIG. 5

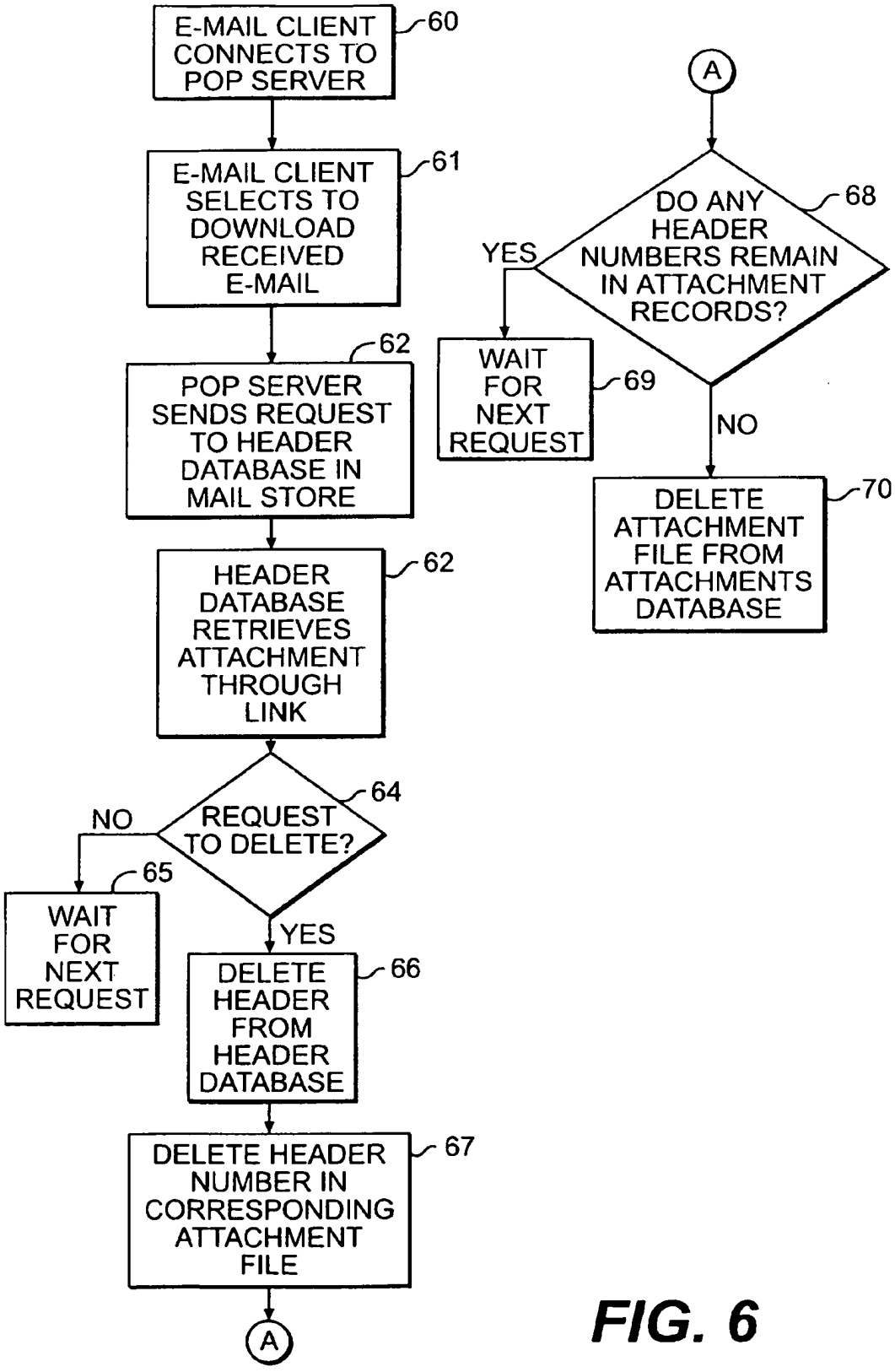

E-MAIL CLIENT CONNECTS TO POP SERVER
60
E-MAIL CLIENT SELECTS TO DOWNLOAD RECEIVED E-MAIL
61
POP SERVER SENDS REQUEST TO HEADER DATABASE IN MAIL STORE
62
HEADER DATABASE RETRIEVES ATTACHMENT THROUGH LINK
62
REQUEST TO DELETE?
64
NO
YES
WAIT FOR NEXT REQUEST
65
DELETE HEADER FROM HEADER DATABASE
66
DELETE HEADER NUMBER IN CORRESPONDING ATTACHMENT FILE
67
A
A
DO ANY HEADER NUMBERS REMAIN IN ATTACHMENT RECORDS?
68
YES
NO
WAIT FOR NEXT REQUEST
69
DELETE ATTACHMENT FILE FROM ATTACHMENTS DATABASE
70

FIG. 6

METHOD AND APPARATUS FOR MINIMIZING STORAGE OF COMMON ATTACHMENT FILES IN AN E-MAIL COMMUNICATIONS SERVER

FIELD OF THE INVENTION

The present invention relates to the storage and maintenance of e-mail attachment files in an e-mail communications server, and more particularly, to a method and apparatus for reducing the number of copies of identical attachment files stored in the e-mail communications server.

DESCRIPTION OF THE RELATED ART

During the past decade, electronic mail ("e-mail") has become an indispensable tool for facilitating business and personal communications. Through computer networking systems such as local-area networks ("LAN"), wide-area networks ("WAN"), and the world-wide web ("WWW"), network users can send and receive notes, messages, letters, etc., to communicate with others who are in the same office or perhaps in remote locations across the world.

E-mail application programs are typically configured for generating messages in the form of memoranda. An e-mail application user interface guides a user to "compose" an e-mail communication by providing a platform for entering at least one outgoing e-mail address, a "subject" heading, and a "body" for the actual message. The user may also designate a document, file or executable program to be attached to the e-mail message. When the user completes typing the message and presses the "send" key, the message is transmitted over the network and is routed for delivery to an e-mail server corresponding to the provided destination address.

A known e-mail communications system and a method for transmitting e-mail communications between networks over the Internet are described with reference to FIG. 1. Computers **10***a*–**10***c* are connected through a local area network (LAN) **11** to e-mail communications system **12**, which can send e-mail communications to any of computers **18***a*–**18***c* through e-mail communications system **16** and local area network (LAN) **17**. E-mail communications systems **12** and **16** include Mail Transport Agent (MTA) servers **12***a*, **16***a*, Post Office Protocol (POP or POP3) servers **12***b*, **16***b*, and Message Store **12***c*, **16***c*. The e-mail communications servers **12** and **16** are also connected to their respective domain name servers (DNS) **13**, **15**.

When an e-mail communication is transmitted according to the Simple Mail Transport Protocol (SMTP), it is first divided into three components: the sender's "mail from:" address; the recipient address list; and the data portion of the message. After a user of computer **10c** prepares an e-mail communication and sends the e-mail across the LAN **11**, it is sent to the MTA **12***a*, which accepts e-mails for delivery. The MTA then separates the address information from the data portion of the e-mail. The MTA parses the envelope to determine whether to route the message to an external network or store the message in Message Store **12***c* for access by another computer connected to the LAN **11**. The MTA "postmarks" the e-mail by adding routing data to the header before storing the message.

If the e-mail is to be sent to another user on a different mail system, the MTA **12** next determines the domain for the intended recipient through its DNS **13**, which queries the recipient system's DNS **15** through the Internet. Upon receiving the domain information, MTA **12***a* transmits the e-mail communication to MTA **16***b*, which is waiting to accept e-mail. MTA **16***b* then stores the received e-mail in Message Store **16***c*. Later, a user on computer **18***a* can log in to the e-mail system and connect to the POP server **16***a*, which determines if there is new mail to download. POP server **16***a* can then retrieve the e-mail communication from the Message Store **16***c* and transmit the e-mail through the LAN **17** to the user.

It is common for users to send a single e-mail communication to multiple recipients. This typically occurs when the e-mail communication contains a humorous joke or anecdote, a political announcement or notice, an advertisement, or pertains to any other subject matter that is of common interest. Some of the recipients may in turn forward this e-mail communication to other groups of recipients. In some instances, a single e-mail communication ultimately may be transmitted and forwarded to thousands of recipients, and, through different sources, some users may even receive multiple copies of the same e-mail communication. Such e-mail communications may additionally include large attachment files stored along with the e-mail message.

When an e-mail communication is transmitted to a plurality of recipients who are connected to the same e-mail communications server, only a single copy of the e-mail communication message and attachment is stored in the Mail Storage of the e-mail server. For example, if a prospective vendor sends a solicitation via e-mail to a large group of employees in a single company, the company's e-mail server will store only a single copy of the e-mail solicitation. The e-mail message and attachment will remain in the Mail Storage until it is designated for deletion by each of the recipients. Consolidating storage of e-mail communications in this manner can reduce the amount of memory required in the company's e-mail communications server.

Although presently available e-mail communications systems consolidate storage when an e-mail communication transmitted by a single sender is received for distribution to a plurality of recipients in a common e-mail server, such e-mail systems do not consolidate storage of the e-mail communication file when it is forwarded to others in the network, resulting in multiple copies of the same file(s). Likewise, if a common e-mail communication is separately transmitted to multiple recipients in a network, or is transmitted multiple times to a single recipient, the e-mail system retains multiple copies of the same file(s) in Mail Storage. This duplication of file storage reduces the efficiency of the e-mail communications server.

SUMMARY OF THE INVENTION

In view of the difficulties described above regarding the duplication of storage of common e-mail communications in an e-mail server, there is a need for a method and apparatus for automatically detecting and consolidating storage of common e-mail attachment files received in an e-mail communications server.

An object of the present invention is to provide a method of storing an e-mail communication containing an attachment file received in an e-mail server. A database of attachment files previously stored in the e-mail server is searched for a copy of the attachment file from the received e-mail communication. If a copy of the attachment file is located in the e-mail server, the attachment file from the e-mail communication is removed, and a link is created from the e-mail communication to the previously stored attachment file in the database.

Another object of the present invention is to provide a method of storing attachment files to e-mail communications received in an e-mail server. Header information from the e-mail communications is extracted and stored in a mail store. Header information from the attachment file to be stored is also extracted. The extracted attachment file header information is compared with header information from attachment files previously stored in the mail store to determine whether the attachment files received with the e-mail communications are duplicates of previously stored files. If an attachment file is a duplicate, a link is stored in the mail store between the e-mail header information and the previously stored attachment file.

Yet another object of the present invention is to provide an e-mail communications server. An MTA server receives e-mail communications from an external network. A mail store stores e-mail communications received by the MTA server. A POP server downloads e-mail communications from the mail store to client computers through an internal network. E-mail attachment file checking software determines whether attachment files in received e-mail communications are duplicates of attachment files in the mail store. The mail store then removes duplicate attachment files from e-mail communications and creates links from received e-mail communications to the corresponding attachment files in the mail store.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. **1** is a schematic diagram of a known e-mail communications and computer network system.

FIG. **2** is a schematic diagram of an e-mail communications server according to a preferred embodiment of the present invention.

FIG. **3** is a flow diagram for storing storing an attachment file in the e-mail communications server of the preferred embodiment of the present invention of FIG. **2**.

FIG. **4** is a table of an exemplary header database in the e-mail communications server of FIG. **2**.

FIG. **5** is a table of an exemplary attachment file database in the e-mail communications server of FIG. **2**.

FIG. **6** is a flow diagram for deleting e-mail communications and e-mail attachment files from e-mail communications according to the preferred embodiment of the present invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

The present invention provides an e-mail communications system that minimizes the number of duplicate copies of common attachment files to e-mail communications that are stored in the mail store of an e-mail server. When the e-mail server receives an e-mail attachment file that is larger than a threshold size, the server performs a database search for another copy of the attachment file in the mail store. If another copy is located, the system creates a pointer in the mail store that associates the located attachment file with the e-mail for the additional recipient(s). An attachment file is deleted only after all e-mail communications that include the attachment file are deleted.

The present invention will now be described in more detail with reference to the figures. FIG. **2** is a schematic diagram of an e-mail communications server **20** in accordance with a preferred embodiment of the present invention. E-mail server **20** includes an MTA server **22** for transmitting and receiving e-mails, a mail store **23** for storing e-mail communications prior to downloading by a recipient client, and a POP server **21** for forwarding e-mail communications from the mail store **23** to recipient clients. In the present invention, e-mail server **20** additionally includes a duplication checker **24**, which intercepts e-mail communication files prior to storage in mail store **23**. The duplication checker **24** contains size checker software **25** that determines the size of e-mail attachments to be stored in the mail store **23**, and file comparison software **26** for detecting whether large e-mail attachment files that are to be stored are duplicate copies of previously-stored e-mail attachment files.

Mail store **23** contains an attachment file storage database **28** for storing attachment files from e-mail communications received from the MTA **22**. The attachment files are stored separately from the corresponding e-mail header information and message, which are maintained in a header database **27**. For each e-mail communication received by the MTA **22** that includes at least one attachment file, the header database **27** stores at least one link to the corresponding attachment file(s) in the attachment file storage database **28**. As explained in further detail below, detected attachment files that are referenced by multiple e-mail communications are stored in a common attachment section **29***a*, separate from the storage of other attachment files **29***b*. Much like a cache, the common attachment section **29***a* stores files that are accessed more frequently in the attachment file database **28**.

FIG. **3** shows a method for storing e-mail attachment files in the mail store according to the preferred embodiment. When an e-mail communication is received in the MTA server in step **30**, the MTA server processes the e-mail communication in step **31** to separate the header file from the e-mail message data and e-mail attachment file data, if present. If the MTA server determines in step **32** that no attachment file is included in the e-mail communication, the e-mail message is stored in step **33** in the mail store. The e-mail message may be stored in any conventional manner in the mail store. The mail store may be configured such that the e-mail header and message are stored in header database **27**, without a link to the attachment file storage database. Alternatively, the header of the e-mail message can be stored in header database **27** with a link to the e-mail message data, which may be stored in another e-mail database in the mail store (not shown in FIG. **2**). As a further alternative, the e-mail header and message data may be stored together in the e-mail database without any link in the header database **27**.

If the MTA server determines in step **32** that an attachment file is included in the e-mail communication, the size checker software **25** in the duplication checker **24** determines the attachment file size in step **34**. If it is determined in step **35** that the attachment file is not greater than a threshold size, the mail store in step **39** stores the header and message information (depending upon configuration) in the header database **27**. In step **40**, the attachment file is then stored in the main section **29***b* of the attachments file storage database **28**. A link is created in the header database from the header to the stored attachment file. In the e-mail server **20** of the preferred embodiment, all attachment files, regardless of size, are stored in the attachment file storage database, and the header database **27** creates a link from the corresponding e-mail header to the attachment. In the alternative embodiment in which the e-mail message is stored in an e-mail database in the mail store **23**, the attachment file may also be stored in the e-mail database together with the e-mail message.

The duplication checker of the preferred embodiment is configured to reduce the number of duplicate attachment files that are greater than a certain, predetermined threshold size. As will be described, the steps of processing the attachment file prior to storage, searching the attachment file database for duplicates, and moving files from the main section **29***b* to the cached common attachments portion **29***a* of the attachment files database are time intensive. Attachment files of a relatively small size, such as those below 50 KB, do not occupy significant space in the attachment file storage database, even if multiple copies have been received and stored therein. Therefore, attachments that are relatively small text files, such as short letters or memoranda, are not searched for duplicates. In contrast, large attachment files, such as those above 1 MB (or any other predetermined threshold), can require significant resources when multiple copies are stored in the e-mail server. An inordinate number of duplicates of large attachment files stored in the e-mail server may overfill the server, such that the e-mail communications server will cease operating until files are deleted. For this reason, information systems managers who operate conventional e-mail communications systems caution users to promptly delete large e-mails and discourage others from sending e-mails with large attachment files to the e-mail server.

If, in step **35**, size checker **25** in the e-mail server **20** determines that an e-mail attachment in a received e-mail communication is greater than a threshold size, the duplication checker **24** next processes the attachment file in step **36** to generate file identification information. As will be described in further detail below, this can be performed by any of several methods, such as a checksum determination, or extraction of certain attachment file header information. The processing step generates information by which the attachment file comparison section **26** of the duplication checker **24** can search the attachment file storage database **28** for identical attachment files, in step **37**.

If the duplication checker determines, in step **38**, that there are no copies of the attachment file previously stored in the mail store **23**, then the mail store stores the attachment file in the main section **29***b* in step **39**, and creates a record in the header database and a link in the record from the attachments database to the header database, in step **40**.

If the duplication checker locates another copy of the attachment file, the mail store **23** checks in step **41** if the attachment file is presently stored in the cache portion **29***a* of the attachment file storage database **28**. However, if the duplication checker determines that the attachment file is in the cache portion **29***a*, then the attachment file is already associated with a plurality of e-mail communications. In that case, the mail store creates a link in the record of the header database to the attachment in the cache portion **29***a* in step **44**.

If the attachment file is not presently in the cache portion **29***a*, then the attachment file has thus far been associated with only a single e-mail communication. In step **42**, the attachment file is transferred from main section of the database **29***b* to the cache portion **29***a*. The links in the record of the other, previously stored e-mail communication associated with the attachment file is modified to reflect the change in storage location in step **43**. The mail store then creates a link in the record of the header database to the attachment in the cache portion **29***a* in step **44**.

In the preferred embodiment, as shown in FIG. **3**, the mail store **38** places an attachment file in the cache portion of the attachment file storage database **28** only when there are a plurality of e-mail communications received that contain an identical attachment file. In some e-mail communications systems, when a sender transmits a single e-mail communication to a plurality of recipients on the same e-mail server, the MTA in the e-mail server receives a single e-mail with a plurality of recipient addresses in the header. For such systems, the mail store **23** can be configured to check, after determining in step **38** that there is not an attachment file already in the database, whether the header of the received e-mail communication contains a plurality of recipients who are on the e-mail server. In such case, the mail store will create a pointer in step **41** and store the attachment file in the cache portion of the database in step **43**.

The process of searching the attachment file storage database **37** for a duplicate of the attachment file to be stored in the mail store indicated by step **37** of FIG. **3** can be performed by a variety of methods, according to the type of information process for file identification in step **36**. Although the most accurate method for determining whether a duplicate file exists in the attachment file database is to perform a bit-by-bit comparison of each file stored in the database with the file to be stored, such a test would be unduly time consuming and would adversely affect the operability of the e-mail system. A more efficient method to identify the attachment files is to compare the characteristics concerning the files, rather than the actual file data itself.

According to the preferred embodiment, the duplication checker **24** first identifies the type of file that is to be stored as an attachment to an e-mail communication. For example, an attachment file may be a text, spreadsheet, graphics, picture, audio, or video file. By searching first according to the type of file, the duplication checker can immediately eliminate the majority of files stored in the mail store from consideration. The duplication checker next identifies the properties associated with the attachment file in the file header, which may include any of: title/name, MS-DOS name, software program, software program version number, author, creation date/time, last modified date/time, size, attributes, last saved by, revision number, and revision time (minutes). In the case of a text document, such as a Microsoft Word™ document, other properties might include the number of sections, pages, paragraphs, lines, words, and characters. A Microsoft PowerPoint™ document may include properties such as the type of fonts used, design template, embedded OLE servers, and slide titles.

The duplication checker searches the properties of each attachment file in the database that is of the same type as the application file in the received e-mail communication. If another attachment file has the identical properties, the attachment file in the received e-mail is identified as being a duplicate.

FIGS. **4** and **5** illustrate an example of the method for storing an attachment file in the mail store. The e-mail server **20** of the preferred embodiment, operating an e-mail system for the domain "anycompany.com," receives an e-mail in the MTA server **22** on Nov. 7, 2000, intended for an employee at the company, Larry Aslad. The MTA server processes the e-mail and identifies the following: the e-mail communication is from debl@anyisp.com; it is to be sent to asla8908@anycompany.com; the subject heading is "This will get you laughing"; the size of the file is 2.03 MB; the e-mail was delivered on Nov. 04, 2000, at 10:22 AM; and the e-mail includes an attachment file. The size of the attachment file is 2.03 MB.

Because the attachment file in the received e-mail communication is greater than the threshold size of 0.5 MB, the duplication checker **24** processes the attachment file in the e-mail communication for file identification. Looking to

header of the attachment file, the duplication checker identifies that the attachment is a video file, entitled "Whassup," playable on Real Audio™, version 2.0, created on Oct. 6, 2000, authored by "Spike."

The duplication checker **24** now performs a search of the attachment file database for common attachment files. Searching the cached attachment file of FIG. **5** first, it becomes clear that there is only one video file stored in the cache, link number **3**. As indicated by the "header number" field, this file is currently the linked attachment for header numbers **1**, **5**, and **6**.

Comparing this file to the attachment file in the e-mail, it becomes evident that the title, size, software and version, author, and creation date are the same.

Based upon these common properties, it is determined that the attachment file in the e-mail communication for asla8908@anycompany.com is a duplicate. It is worth noting that the subject headings for the e-mails stored as header numbers **1**, **5**, and **6** are each different, and header number **5** was received on a different date from a different source than headers **1** and **6**. The duplicate server and mail store can detect that the attachment files are duplicates by storing the attachment file separately from the corresponding e-mails.

Because the file is already in the cache portion of the database, there is no need to move the attachment file from the main attachment file storage database **29***b* to the cache **29***a*. The mail store **23** creates a new link and header record in the header database of FIG. **4**. The new header record appears as follows: header no. **9**; username asla8908; subject "This will get you laughing;" date received Nov. 7, 2000, and from deb1@anyisp.com. Attachment "3" corresponds to the previously cached storage of the same file in the mail store. In the cached attachment files, header no. **9** is now added to the header number list.

The steps for retrieving e-mail from the e-mail server by a client computer are now described with reference to FIG. **6**. An e-mail client connects with POP server **21** in step **60**, and selects to download received e-mail in step **61**. The POP server then accesses the header database **27** in the mail store in step **62** and extracts the header and e-mail message information from the mail store. In step **63**, the mail store retrieves the attachment file corresponding to the requested e-mail communication through the link in the header database to the attachment file storage database **28**. The client now can view, reply, forward, copy, or delete the received e-mail message and corresponding attachment file.

If the POP server detects in step **64** that the client requests to delete the e-mail communication, the header in the mail store corresponding to the received e-mail communication is deleted from the header database in step **66**. The header reference number is then deleted in step **67** from the corresponding attachment file in the attachment file storage database. The mail store then checks in step **68** if any header reference numbers for the attachment file remain in the attachment database. If all e-mail recipients have deleted the e-mail communication, then the attachment file is deleted from the attachment database, in step **70**.

Accordingly, the duplication checker and mail store header and attachment databases of the present invention can minimize storage of duplicate attachment files in an e-mail communications system. The e-mail server of the present invention is configured such that duplicate copies of attachment files are not unnecessarily stored in the mail store, whether the attachment files are received through separate e-mails or e-mail forwarding by users within the same e-mail server network. Thus, it is readily seen that the method and system of the present invention provides for improved and efficient e-mail communications, and saves valuable memory space in the mail store of an e-mail server.

The foregoing disclosure of embodiments of the present invention and specific examples illustrating the present invention have been presented for purposes of illustration and description. It is not intended to be exhaustive or to limit the invention to the precise forms disclosed. Many variations and modifications of the embodiments described herein will be obvious to one of ordinary skill in the art in light of the above disclosure. The scope of the invention is to be defined only by the claimed appended hereto, and by their equivalents.

What is claimed is:

1. A method of storing attachment files to e-mail communications received in an e-mail server, comprising:

responsive to the e-mail server receiving an e-mail communication containing an attachment file, the e-mail server extracting header information from the e-mail communication and storing the e-mail header information in a mail store;

the e-mail server extracting attachment file header information from the attachment file contained in the e-mail communication;

the e-mail server comparing the extracted attachment file header information with attachment file header information from other attachment files previously stored in the mail store to determine whether the attachment files received with the e-mail communications are duplicates of previously stored files;

if an attachment file is a duplicate, the e-mail server storing a link in the mail store between the e-mail header information and the previously stored attachment file; and

then the e-mail server removing the attachment file from the e-mail communication.

2. The method of storing attachment files to e-mail communications according to claim **1**, further comprising:

if an attachment file is not a duplicate of a previously stored attachment file, then storing the attachment file in the mail store and storing a link in the mail store between the e-mail header information and the attachment file to the received e-mail communication.

3. The method of storing attachment files to e-mail communications according to claim **2**, further comprising:

deleting the e-mail header information stored in the mail store and the link

between the e-mail header information and the corresponding attachment file in response to a delete request; and

deleting the corresponding attachment file if there are no links remaining to the attachment file.

4. The method of storing attachment files to e-mail communications according to claim **1**, wherein e-mail messages in the e-mail communications are stored with the corresponding e-mail header information in the mail store.

5. The method of storing attachment files to e-mail communications according to claim **1**, wherein the header information extracted from the attachment files includes a designation of file type.

6. The method of storing attachment files to e-mail communications according to claim **5**, wherein the step of comparing extracted attachment file header information is performed by searching the previously stored attachment files that are designated as the same file type as the attachment file to the received e-mail communication.

7. The method of storing attachment files to e-mail communications according to claim **5**, wherein the header

information extracted from the attachment files further includes at least one of: size, creation date, revision date, author, software type, version, and revision number.

8. The method of storing attachment files to e-mail communications according to claim 1, wherein the step of comparing extracted attachment file header information is performed only when the size of the attachment file is greater than a predetermined size.

9. An e-mail communications server comprising:

an MTA server for receiving e-mail communications from an external network;

a mail store for storing e-mail communications received by the MTA server;

a POP server for downloading e-mail communications from the mail store to client computers through an internal network; and

e-mail attachment file checking software for determining, responsive to the MTA server receiving an e-mail communication containing an attachment file, whether the attachment file in the received e-mail communication is a duplicate of an attachment file that was attached to previously-received e-mail communications in the mail store,

wherein the mail store removes duplicate attachment files from e-mail communications and creates links from received e-mail communications to the corresponding attachment files in the mail store after the e-mail attachment file checking software determines that the attachment file in the received e-mail communication is a duplicate of an attachment file in the mail store.

10. The e-mail communications server according to claim 9, wherein the mail store further comprises a database for storing the links from received e-mail communications to the attachment files.

11. The e-mail communications server according to claim 10, wherein the mail store further comprises a first attachment storage database for storing attachment files that are each associated with a single e-mail communication, and a second attachment storage database for storing attachment files that are each associated with a plurality of e-mail communications.

12. The e-mail communications server according to claim 9, further comprising e-mail file attachment size checker software for detecting the size of attachment files in received e-mail communications, wherein the e-mail attachment file checking software only checks attachment files that are greater than a predetermined size.

13. The e-mail communications server according to claim 9, wherein the e-mail attachment file checking software extracts properties associated with the attachment files in the received e-mail communications, and searches the mail store for attachment files having the same properties.

* * * * *